CYBERSECURITY IN ENGINEERING AND TECHNOLOGY

CYBERSECURITY IN ENGINEERING AND TECHNOLOGY

NATARAJAN R

ISBN - 978-93-92423-06-2

Cybersecurity in Engineering and Technology

Natarajan R

First published in India 2022 by

FRATECLAT PVT. LTD.

Cherry Publications India

Aligarh, Uttar Pradesh (202001)

Printed at Sanjay Printers, Sahibabad, India

To find out more about our authors and books visit

www.cherrypublications.com

Email: info@cherrypublications.com

Content Table

CHAPTER 1

ETHICS IN CYBERSECURITY

The increasing use of information and communication technology (ICT) in all spheres of modern life makes the world a richer, more efficient and interactive place. However, it also increases its fragility as it reinforces our dependence on ICT systems that can never be completely safe or secure. Therefore, cybersecurity has become a matter of global interest and importance. Accordingly, one can observe in today's cybersecurity discourse an almost constant emphasis on an ever-increasing and diverse set of threat forms, ranging from basic computer viruses to cybercrime and cyberespionage activities, as well as cyber-terror and cyberwar.

This growing complexity of the digital ecosystem in combination with increasing global risks has created the following dilemma: Overemphasizing cybersecurity may violate fundamental values like equality, fairness, freedom, or privacy. On the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure as well as in policy makers and state authorities. The goal of this Chapter is to show how the ethical discourse on cybersecurity has developed in the scientific literature, which ethical issues gained interest, which value conflicts are discussed, and where the "blind spots" in the current ethical discourse on cybersecurity are located. The Chapter is based on an extensive literature with a focus on three reference domains with unique types of value conflicts: health, business/finance and national security. "Ethics and cybersecurity" is not an established subject, academically or in any other domain of operation. It is actually a rather under-developed topic within ICT ethics, where the majority of published work discusses issues such as "big data" and privacy or ethical issues of surveillance.

In those cases, cybersecurity is usually only instrumentally discussed as a tool to protect (or undermine) privacy. Nevertheless, cybersecurity raises a plethora of ethical issues such as "ethical hacking", dilemmas of holding back "zero day" exploits, weighting data access and data privacy in sensitive health data, or value conflicts in law enforcement raised by encryption algorithms. Those issues are in most cases discussed without the claim to gain an integrative view on the ethics of cybersecurity.

Hence, the goal of this Chapter is twofold: first, to identify the emerging landscape of ethical issues, concerns, and topics as they are mentioned in the literature, and, second, to provide a value framework as both a philosophical compass and synthetic portray of the emerging ethical issues. The target audience of this Chapter is not only the philosophy and ethics of technology community, but also practitioners in cybersecurity – such as providers of security software, CERTs or Chief Security Officers in companies. All those people increasingly realize the ethical dimensions of their work. This Chapter should provide a first orientation in the growing landscape where cybersecurity and ethics meet.

In 2008, the International Telecommunication Union (ITU) defined cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability, integrity and confidentiality of systems and data, which may include authenticity and nonrepudiation"

Another key term in this Chapter is "ethical issue". By this term, we denote any instance of a real world effect of a certain cybersecurity measure, policy, action etc. that has been described using an ethics terminology. By "describing" we mean that this instance has been regarded as a measure thateither helps to enforce or protect an ethical value, norm or virtue, or that this instance is endangering or in conflict with an ethical value, norm or virtue. The notion of an "ethics terminology", respectively "ethical" value, norm or virtue is not precisely defined in the literature.

Referring to the huge literature body in moral philosophy and research in empirical ethics , people associate ethical values (norms, virtues, etc.) usually with something that claims to be universally valid and whereas its corresponding actions are judged as right or wrong (philosophical dimension of morality; setting aside moral relativism), that usually refers to the goals of a community, common interest or the relationships among individuals (social dimension of morality), and that often refers to the collaboration, cooperation or communication between human beings or institutions . In the following, we will use those characteristics as "markers" for ethical issues.

Yet another key term in this paper is “value”, that we take here as the standard point of reference with respect to an ethical orientation (i.e., we will not use the notion of “norm” or “virtue”, although some instantiations of what we call “value” in this Chapter can reasonably also be called a “norm” or in some cases even a “virtue”). In very general terms, we denote by ‘‘value” any term that individuals or institutions consider being a positive goal worthy of achievement.

For example, profit is a positive orientation in business and beauty is a positive one in art. Certainly, not all those positive orientations are ethical values – those would be values where we reasonably can assume that they are in line with the characterizations.

1.1 CYBERSECURITY IN HEALTH:

In Western culture, at least since the time of ancient Greece, there has been a great deal of thought given to the value of health for a successful life. It is not for nothing that the Hippocratic Oath still refers to the eponymous physician and philosopher, even though he lived almost 2500 years ago. Epicurus, who lived in the third century B. C., also gives us thoughts on the importance of health. This thinking continues to this day. It is probably no exaggeration that health, despite all the problems of a precise definition, enjoys high priority in all cultures.

Therefore, in order to protect health, the WHO has formulated the right to health as a central human right. If one agrees that health is an important, if not most important, value to human beings then a health care system that can provide effective and efficient help in case of medical problems also is most valuable. In this Chapter we will not discuss questions of justice with regard to health care and we will also not discuss the benefits and burdens or the moral justifications of the different ways to maintain and finance an effective and efficient health care system. However, such a health care system needs resources and providing these resources is becoming more difficult. As Nancy Lorenzi puts it, currently almost every major economy in the world experiences the effects of the high cost of health care, and many, if not most, national and regional governments are in some stage of healthcare reform.

In many, if not almost all, attempts to reform an existing health care system, the development and implementation of information and communication technology (ICT) to support the provision of health care services is a major part of those reforms. One of the

main purposes of ICT systems in health care is the administration of information about patients and treatments that is a vital but complex component in the modern health care system. At a minimum, health care providers need to know a patient's identity and demographic characteristics, recent and distant medical history, current medications, allergies and sensitivities, chronic conditions, contact information, and legal preferences

McClanahan also stresses that the increased use of electronic medical records has created a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain. Employing ICT in health care therefore creates new value conflicts or at least makes old conflicts and problems more visible or increases their urgency. At the same time, it has to be stressed that improvements in the health status of communities depend on effective public health and healthcare infrastructures. These infrastructures are increasingly electronic and tied to the Internet. Incorporating emerging technologies into the service of the community has become a required task for every public health leader.

In other words, stakeholders like patients, health care professionals, health care providers, or insurance companies as well as societies as a whole are confronted with competing or even contradicting aims with regard to the health care system, for instance:

- increasing efficiency

- reducing costs

- improving quality

- keeping information secure.

Simultaneously, the moral values mentioned above also shall be protected and supported, either as fundamental moral values in European societies and/or as moral values, which are constitutive for the relationship between patients on the one side and health care professionals on the other side. Such conflicts of aims and values raise moral concern since it has to be decided which aim and which value should be prioritized.

In fact, the situation is even more complicated because there are not only the above-mentioned conflicts, but also medically related conflicting goals and values. One example is the conflict between beneficence and autonomy: When ICT is used in the health sector, it shall be aimed at ensuring that patients themselves determine when which information

is revealed to whom – password protection and encryption are common measures to maintain that aim. However, in emergencies, when patients are no longer able to make this decision, there is now a risk that important medical information will no longer be accessible.

Moreover, it might be very helpful to widely share medically relevant patient information among health care professionals to improve the quality and efficiency of treatment. However, the goal of protecting patients' privacy and autonomy may be at odds with this aim. Additionally, as the literature search described below shows, in scholarly debates it is often mentioned that to provide cybersecurity it might be necessary to compromise privacy. This raises particular concern, because it is obvious that both the protection of patients' privacy and the security of information systems and the patient data organized in them must be important objectives in health care. Without privacy, the confidence necessary for medical treatment is jeopardized and without certainty that patient data will not be tampered with or stolen, the treatment itself is at risk.

The majority of this chapter discuss health related electronic information, more precisely the storage, exchange and usage of patients' (big) data. Above all, that requires electronic information databases such as Electronic Healthcare Records (EHR), which are increasingly implemented in health facilities. The major advantage of these records, besides cost efficiency, is the fast and uncomplicated exchange of health related data between organizations. The employment of electronic information is diverse: It plays, for example, an important role in the emergency department or is used in connection with maternal and child health registries. Furthermore, electronic health information has a seemingly big impact on counselling and psychological therapy. The use of electronic data is changing the relationship of patients and health professionals. Many papers address security and privacy problems regarding EHR In those papers, different approaches of how to deal with security and privacy could be identified: particularly, that includes technical solutions such as biometric authentication, secure systems and ethical guidelines.

The moral character of cybersecurity involves protecting data information from harm. We address reoccurring ethical issues in order of which the arise in the literature; i.e., the most frequently occurring topic is discussed first and so on. We firstly address the issue of data/information (used interchangeably) security in which we address the most discussed ethical issues such as protection of information, privacy, threats, insider attacks, trust and so forth. We separately discuss ethical issues that arise in cloud computing mentioning the security risks and benefits associated with adopting to the cloud. The usefulness of ethical

codes appeared in a number of resources and their application in managing cybersecurity in business is addressed.

Hacker ethics and the rationale behind self-identified hackers is then discussed closely followed by cybersecurity issues in e-banking. Lastly, we discuss some literature that focused on the responsibility of corporations to protect personal data from security breaches highlighting the lack of consumer transparency as to how their personal information is used, mined, analyzed and collected by businesses and their third party partners. This literature specifically referred to interoperability applications used by social networking sites which we briefly discuss from an information and data security perspective.

Data & Information Security: Information security raises ethical problems when security breaches occur. Security breaches in business can involve a breach to security resources or information security. Resources such as hardware or software can be damaged or corrupted causing a loss of service, time and money for a business. When information security is breached, this can cause an economic loss for a business but in cases where data is lost, stolen or modified that contains personal, cultural or social value this can cause psychological or emotional harm for the client and consumer. An information security breach may be more detrimental for one business than another. For example, a law firm contains highly valuable data including corporate records, personal information relating to clients, intellectual property and trade secrets thus substantiating a duty on lawyers to use reasonable and adequate cybersecurity measures to prevent unauthorized access to client data as an information breach may threaten the very survival of the firm.

As securing private information is a core aspect of cybersecurity, privacy is valuable to the business and consumer. Privacy protects individuals from external threats such as defamation, harassment, manipulation, blackmail, theft, subordination and exclusion. Walters argues that a threat to privacy is a threat to personal integrity. Definitions of privacy in respect of cybersecurity range from privacy being a fundamental human right, to a necessary condition for autonomy , to an articulation of the core value of security which is meant to protect people from all kinds of harm done by others. In respect of security of private and personal information, Schoeman states: “A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body”. This suggests that protecting the privacy of an individual in the cybersphere encompasses securing the processing of personal information, including technologies that may observe and interfere with human behaviors and relations and their body and their personal belongings.

Sharing Personal Information: It could be argued that businesses who benefit from processing, storing and analysing personal information have an ethical obligation to adequately secure their data. For example, businesses that utilize and benefit from data mining techniques (a tool that enables a company to analyses an individuals' behavior and uncover patterns and information not previously known which may be considered confidential or private; include financial services, consumer products, manufacturing, the pharmaceutical industry, technology/services, retail, telecommunications, energy, and transportation.

Furthermore, businesses that couple data mining technologies with Open Application Programming Interfaces (API), such as social networking sites, may too have an ethical obligation to provide adequate security measures to protect valuable data as such techniques have been said to have "unforeseen ethical consequences". For example, the social networking giant Facebook uses both aforementioned tools enabling its users to navigate from site-to-site and comment, cross-post, "Like", and recommend something to another member, while Facebook tracks, traces and disseminates the members personal information (including "name, profile picture, gender, networks, user ID (UID), list of friends…") with articulated networks and with third-party sites and services.

Bodle argues that there is a lack of transparency and a loss of control for users as they are unaware as to what information is being collected, and how this information is being used, inevitably undermining privacy, data security, contextual integrity, user autonomy and freedom. Other tools include Facebook's Open stream (which allows outsiders to access a user's entire Facebook real-time activity stream) and Instant Personalization Pilot Program (which allows third party access to members' data from which third parties can tailor content to the user's tastes respectively). These tools require enhanced security such as authentication preventing anonymity and inhibiting free movement online.

Biletzk's makes the argument that the very concept of "security, whether on line or not, is a rhetorical instrument in the hands of interested parties…". Bodle acknowledges that soliciting members data flows increases data portability and tailoring personalized content is drawn from information emanated from the individual themselves, however he makes the argument that the extensions of these techniques are used at the expense of user autonomy. Bodle further notes that members lack of awareness inhibits individuals' ability to make informed decisions thus relinquishing self-determination and suggests a more humancentric business approach based on values and principles including transparency, privacy, security, autonomy, and user control as alternatives to various forms of market enclosure.

Control of Information: As security must protect the purpose of data processing and the actual data processing, some argue that failing to strike a balance between the two affords cybersecurity the potential to promote or inhibit the safety, security, privacy and civil liberties of individuals and organisations . One purpose of data mining can be to stereotype whole categories of individuals. Conger argue that ethical conflict arises when the individual has not given informed consent for this type of analysis of their private data whether it takes place before, during or after a transaction is complete. Whether informed consent is obtained for data to be shared with third party partners should be raised, as the individual may be unaware that once shared the personal data is no longer controlled by its first and second party donors. Dean analyse data mining from the Golden Rule's perspective – one should do unto others as he would have others do unto him – and suggest that data miners ought to consider three moral requirements:

1) that the actor treat all acted upon equally and in like manner to action he would accept

2) that the person acted upon be regarded as inherently valuable and not just as a tool to attain the actor's own ends

3) that freedom of the person acted upon be respected. In doing so, the first looks at how information is collected, stored online and/or shared with others, the second considers how the collection or use of data benefits the data subject and the third commands the data miner to acknowledge and respect the autonomy of all rational beings.

1.2 INFORMATION AVAILABILITY IN CYBER SECURITY:

Van den Hoven argues that access to information has become a moral right of citizens in the information age because information has become a primary social good: a major resource necessary for people to be successful in society. The high availability rates of the internet and online storage, enable businesses to readily use on-demand services in the form of cloud computing. However, high availability comes with security risks during the process of transferring information between parties. Responsibility and accountability issues can also be a concern as it is unclear whether data is secured at all times and whom takes responsibility for the maintenance and backup of the information held in the cloud.

Locating data due to the practice of data replication in the cloud can also prove very difficult as the system in use may automatically replicate data to different locations all across the world. This raises a further security, ethical and potentially legal issue as data might be lost or stolen in a country where legislation on data protection and information security is

not as stringent as the host's country. Pearson suggests that security need not suffer in moving to the cloud as outsourcing security to security experts can provide greater protection than previously obtained – the key is to select suitable service providers who have controls in place that respect privacy and are context-dependent.

Control in the Cloud: Cloud computing is a common business tool used by corporations that can be vulnerable to both outside and insider threats. The cloud enables businesses to reduce operational costs bypassing the need for an in-house IT department and renting the infrastructure from their provider, relieving the businesses from buying the hardware themselves. However, the ease and efficiency of the cloud comes with privacy risks and the issue of control over data processing as customer's data is processed remotely in unknown machines. Pearson argues that there needs to be an appropriate level of access control within the cloud environment to protect the security of resources as cloud computing may increase the risk of access to confidential information. Control over the infrastructure is available in five formats: public, private, hybrid, managed and community-owned. This is indicative, as it can be unclear as to who controls the information and infrastructure, and who owns it . For example, in a managed cloud, a company owns its own IT infrastructure but outsources the management to a third party. In the case of public clouds, they are owned and managed by third parties and are possibly accessible to anyone including competitors and are the most challenging when it comes to security. Therefore choosing the most suitable cloud to meet the businesses needs and, in addition, to ensure adequate security for the protection of the business, client and consumer is important. Most corporations utilise a hybrid cloud where they host most of their insensitive applications and data in the public cloud and secure their sensitive data and application in an in-house built private cloud. \

Kouatli proposes that "special cloud ethics" needs to be developed "to maintain an ethical and secure environment for the service providers' clients". Closely related to the control issue is responsibility in the cloud. Responsibility can be a challenge in cloud computing in respect of which parties are responsible for which aspect of security. A number of threats coincide with cloud computing such as abuse and nefarious use of cloud computing, insecure interfaces and APIs, malicious insiders, shared technology issues, data loss or leakage and account/service hijacking.

Pearson (2012) notes that if entities are involved in the provider chain that have inadequate security mechanisms in place, this can exacerbate the problem of unauthorised access. Nothing that the potential damage caused in the cloud is greater than non-cloud environments due to the scale of operation, the presence of certain roles in cloud

architectures and the fact that data may remain in the cloud for long periods of time often results in a greater exposure time for an attack. De-perimeterisation is the fading of the boundaries of organizations and their information infrastructure, which can raise similar control issues in the cloud. It is noteworthy to mention that de-perimeterisation can also be an issue when businesses hire consultants from third parties or allow employees to use mobile devices as such structural changes to an organization challenge the containment-based approach to information security and force organizations to implement data-level security instead.

Cost & Data Quality: Structural changes such as offshoring and outsourcing can also raise some concerns. For example, in financial institutions security and privacy are the main risks associated with offshore outsourcing, as security breaches at offshore locations are harder to detect where "ensuring physical protection of data at a foreign site is more difficult than doing so at a local site". Poor data quality in the cloud can also be an issue. When data is of poor quality this has two implications; the first is that the security of an enterprise becomes compromised as security is directly linked to the accuracy of data. The second is that usability of a system comes into question if the system and data therein are not useful or if the data is out of context. This typically results in a loss of ownership and very serious security problems. Quality of data and information security are viewed as value-based issues, which vary in their moral intensity and can have a significant effect on ethical decision-making.

It is argued that investors view offshore/outsource decisions more favorable than consumers on the basis that investors perceive it as a means to improve profitability and firm competitiveness while consumers will have concerns over product safety, service quality and data security. Business ethics scholars substantiate the issues of quality and data security as ethical issues based on the mere obligation that a business has to keep customer information in confidence as well as ensuring product safety. Trevino and Nelson characterise these problems as ethical issues as they "involve obligations to primary or key stakeholder group", which includes the consumer, shareholders, employees and the community. The decision to offshore or outsource is discretionary and affects the lives and wellbeing of others leading Trevino and Nelson to the conclusion that offshoring is a moral issue as it is an action made with volition which has both beneficial and harmful consequences for others.

Codes of Ethics: In terms of managing ethical issues in relation to cybersecurity in the business domain, corporations can construct rules of conduct and codes of ethics to clarify responsibility and deter unethical behaviors. Codes of ethics ("Code") keep employees

abreast of laws and regulations and clearly outline unacceptable or illegal behaviour and in the absence of a Code, it is easier to rationalise irresponsible behaviour . Pearson and Wiener argue that rationalisations are a way of neutralising the norms generally embraced by an individual, allowing the individual to drift into unethical behaviour . Codes can be the basis for internal sanctions that have a deterrent effect and can thus affect an employee's intentions.

Assuming that they have an impact on the decision-making process of the employee, they can contribute to any one of the following:

(i) increase awareness that an ethics issue exists and a potential computer abuse can occur;

(ii) aid the employee in making a judgment about right and wrong by clarifying right or wrong behaviour regarding the abuse

(iii) encourage employees to abide by their judgments to place the value of doing right above other values and establish ethical intentions for behaviour; and combining points (i) through (iii) cause the employee to behave in an ethical manner. In saying that, codes have received criticism for being used as a public relations gimmick or a means for protecting the corporation from legal liability with some researchers noting that codes lack much impact. Codes have also been accused of being nothing more than pseudo-ethics as they simply codify existing rules and standards of behaviour and do not encourage ethical reasoning when an individual is faced with new or difficult issues such as those which confront IS personnel.

Informed Consent: The requirement for businesses to obtain informed consent from individuals in respect of how organizations store, use or exchange personal and private information emanates from the principle that a person should not be used as an instrument for advancing some goal, but should be fully informed and have freely consented to engage in an activity wherein their interests are respected. This approach entangles the value of trust, which can be viewed as a consequence of progress towards security and privacy objectives as trust revolves around the "assurance" and confidence that people, data, entities, information or processes will function or behave in expected ways. When trust is undermined, a power struggle emerges wherein one party has more power than the other. This reiterates previous arguments that encourage businesses that engage with technologies that process personal data to implement adequate cybersecurity measures that balance individual privacy with corporate use of data security.

Hacker Ethics: A significant difference appears to exist between insider attacks from for example, a disgruntled employee who seeks revenge on their employer, and an outsider attack from for example, a hacker who seeks to reveal information, which will identify problems in systems and cause no harm to institutions. A typical approach among hackers is the belief that by gaining unauthorized access into a system, they are providing a good outcome for the information security community as they believe that all information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world. Tavani counter-argues each point respectively noting that the ideal of information being free undermines privacy, integrity, and accuracy of information (as it could be freely modified at will) and states that information cannot be free as this runs counter to the very notion of intellectual property and would imply that creators of information have no right to keep information to themselves nor have the opportunity to profit from it. Tavani argues that the helpfulness of hacking pointing out security weaknesses may not outweigh the harm it causes as activities in cyberspace do inflict harm in the real world. The code of ethics of Nightmare includes the following statement: "Never harm, alter or damage any computer, software, system, or a person in any way" and if the damage is done, the hacker should do what is necessary to correct the damage and prevent it from occurring again. Leiwo & Heikkuri suggest that hackers see themselves in a similar light to how the Greek philosopher Plato saw himself as the hacker is attempting to achieve something that goes beyond information systems which is similar to Plato's differentiation between one person's love of wisdom and another person's love for knowledge noting "vulgar curiosity does not make a philosopher". In contrast to hacker ethics, information security specialists tend to deontologically specify what ethical behaviour is. From a deontological perspective, virtue is seen as an end of ethical activities. In contrast, hackers tend towards consequential ethics.

According to consequential ethics, the nature of what is done is not essential but the value of activities is determined by the outcome, and virtue is seen as a means to achieve the desired good outcome. Leiwo & Heikkuri's research acknowledges that cultural relativism plays a role in cybersecurity ethics because each judgment is based on personal values informed by the individual's culture. They argue that hacker ethics and information security ethics result from different cultures. Moral agents in these scenes are thus incapable of judging each other's values.

Usability: Bruce Schneier states, "The more secure you make something, the less usable it becomes" suggesting conflict arises when security and usability are not considered collectively. Research indicates that most users prefer usability over security, particularly

in the context of graphical passwords . In relation to the use of secure emails, users prefer integrated solutions where neither security nor usability are compromised. Usability problems within a systems security context include authorization of entities, definition of a security policy for a resource, revocation of rights, checking validity of a set of credentials, privacy of users and distinguishing trusted channels. Privacy enhancing technology (PET) are technical and organizational concepts that aim at protecting personal identity and usually involve encryption in the form of digital signatures, blind signatures or digital pseudonyms (Walters 2001). Walters argues that these technologies may promote and protect privacy and security rights and suggests that smart cards and biometric technologies can utilise PETs in ways that protect privacy and thus human freedom and well-being.

Biometrics: Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioural characteristic. For example, a person can be recognized by traits such as fingerprints, hand geometry, signature, retina or voice. It can be a reliable method of access control and personal identification for organizations such as financial institutions however there are a significant number of security threats in implementing biometric technologies such as the following: changes in lighting and photo angles in face recognition affect the reliability of data; masking a finger to avoid a match in fingerprint technology can affect the validity of matching accuracy; hijacking of contour data in palm scanning/hand geometry could affect confidentiality and privacy; inability to execute liveliness testing in iris/retina scanning opens the potential to print iris patterns on contact lenses; and signature recognition can threaten data accuracy and reliability due to variable trait data.

There is also a risk with privacy and confidentiality if biometric information is stolen or is misused. Thus moderating cybersecurity of biometrics is not just an operational challenge but also an ethical challenge for businesses. There is also the potential for the monitoring organisation to trace the movements and actions of individuals exposing insights into individual behaviour, which may be leaked or used against the individual in the future. A paradox exists at the heart of biometrics as on one hand the technology can be a threat to privacy as it is a technology of surveillance. On the other hand, biometric technologies can be utilized as security mechanisms that protect privacy. A trade-off also exists between usability and security, as users could be greatly inconvenienced trying to update their biometric data if fault tolerant procedures are not in place. The widespread use of biometrics could also have the undesirable effect of eliminating anonymity and pseudonymity in daily transactions, as individuals would leave traces of themselves everywhere they went.

Considering a large percentage of security breaches go undetected, it is likely that figures released by industry surveys regarding computer crime underestimate the actual level of insider information systems misuse. Commentators note that businesses do not report illegal activity to law enforcement or impose severe sanctions on computer abusers. Reporting is shunned, prosecution is complex, detection is uncertain, conviction is rare and rewards such as golden parachutes and well-paid consulting jobs are made available to convicted computer criminals. The effect is that computer abusers are rarely caught or punished - a fact well-known by potential computer abusers.

New technologies such as ubiquitous computing involve the movement from the single workstation and entail embedding microprocessors into everyday working and living environments in an invisible and unobtrusive way. Ambient intelligence is an advanced form of ubiquitous computing as it incorporates wireless communication and intelligent user interfaces that use sensors and intelligent algorithms for profiling. This entails the recording and adapting to user behaviour patterns and involves context awareness to adapt to different situations. In order for ambient intelligence to function, it requires possibly hundreds of intelligent networked computers that are aware of an individual's presence, personality and needs enabling the technology to perform actions and or provide information based on the perceived needs. Securing this technology and data from criminals while also endeavoring to protect the privacy of the individual may prove extremely difficult as dozens of smart devices record activity and are connected to the developers' computers as well as third parties.

Security Breaches & Confidentiality: Businesses have adopted the use of technologies in the cybersphere that aid user access. Corruption or damage to technological resources causes harm in the form of loss of service, time and money. Data lost, stolen or modified can result in a breach of confidentiality, integrity and availability for both the business and the user. For the consumer, this can invoke psychologicand emotional harm. As privacy is a condition of autonomy and is viewed as a core principle of security, a threat to privacy is a threat to not only data security but also data integrity.

Security, Transparency & Control: As there is no consensus on the ethical aspects of information security, the law enforcement is taking the role of providing guidelines on ethical behavior. In order to fight computer fraud research suggests that transparency must be increased within businesses and within society as a whole as this will enable the general public to better understand and manage cybersecurity breaches and simultaneously reduce the excessive control currently held by security departments. In respect of sharing information in cyberspace, there is a lack of transparency as to how data is being used by

businesses and their third party associates. This results in a loss of control for the consumer undermining privacy, security, contextual integrity, autonomy and freedom. Surrendering privacy is the cost of social online engagement despite access to information being considered a moral right. The risk of privacy invasion increases in the cloud as locating data breaches can be difficult especially when data is automatically replicated to unknown locations. A lack of awareness over data use also relinquishes self-determination and inhibits the ability to give free, informed consent. While sharing increases portability and personalized content it also undermines privacy. Certain sharing tools require enhanced security (authentication) preventing anonymity and inhibiting free movement online.

Security Compliance, Costs & Benefits: In relation to the cloud, Pearson (2012) argues that cloud usage is a question of trade-offs between security, privacy, compliance, costs and benefits wherein trust and transparency play a significant role. Further stating that privacy and security issues need to address a combination of issues including the speed and flexibility of adjustment to vendor offerings, which brings benefits to business and motivates cloud-computing uptake but also brings a higher risk to data privacy and security. Cloud technologies enable businesses to reduce costs, but while information is being transferred, it is unclear who is accountable and ultimately responsible if data is lost, stolen or misused.

Access, Privacy & Data Integrity: Hacker ethics promotes the free flow of information with unlimited access to computers advocating that this does not cause harm to the real world. This is in conflict with privacy, as well as integrity and accuracy of information. Information being free is in direct conflict with the notion of intellectual property. In contrast, information security experts base their actions on their duty to act ethically whereas the hacker believes the value of actions is determined by the outcome.

Security, Profit & Data Accuracy: A businesses choice to offshore or outsource activities is a moral issue as it has both beneficial and harmful consequences. Offshoring improves profit and competitiveness but increases the risks of a cybersecurity breach, which is often difficult to detect in a foreign state. There is a greater risk that data will be of poor quality and accuracy, which effects security as security, is based on data accuracy. Usability of data is thus decreased if data is out of context resulting in a loss of ownership and a potential breach of confidentiality. As data quality and security have a moral intensity, the aforementioned issues can affect the wellbeing of others.

Consent & Trust: Consent is inherently linked to trust, and providing security in the business domain entails respecting others by being fair, just and avoiding harm and

dishonesty. A power struggle pervades when actions are not morally balanced. Surveilling employees in the interest of protecting the business comes at the expense of the employee. Surveillance can be in conflict with privacy when consent has not been obtained. This violates the notion of justice on the basis that expectations of fair treatment such as respect, dignity and rights to interpersonal space are not met. The impact of codes of ethics on reducing cybercrime in business is unclear. However, they can clarify responsibilities, outline punishments for unacceptable /unethical behaviour and increase awareness and aid decision making.

Security, Acceptability & Usability: Critics argue that an assumption of ethics as the foundation for security is far too optimistic and cannot be enforced due to the heterogeneity of public networks but note that ethics can be enforced within groups that agree upon common ethical norms and terms of acceptable usage of information systems. The motivating factors could be common business interests and on the individual level driving factors could be terms of employment or codes of conduct within the peer group. Leiwo & Heikkuri suggest an ethics negotiation phase (where organisations negotiate the content of ethical communication agreement over specific communication channels) and an ethics enforcement phase (where each organisation enforces changes in ethical codes of conduct by specifying administrative and managerial routines, operational guidelines, monitoring procedures and sanctions for unacceptable behaviour.

Reliable ICT networks and services are since long a critical element in ensuring public welfare, economic stability, law enforcement, and defense operations. In addition to the health and business domains, malicious attacks on the Internet, disruptions due to physical phenomena, software and hardware failures, and human errors all affect the proper functioning of essential public services that rely on public ICT networks. Such disruptions reveal the increased dependency of our society on these networks and their services. In the national security sphere, however, state actors like the police, and national security agencies have privileged access to ICT services. While this may be needed for law-enforcement, defense operations and counter-terrorism and therefore may increase security, at the same time it might endanger values like freedom and privacy.

Although value conflicts with respect to cyber security in the national security domain are regularly phrased in terms of security versus privacy, at closer inspection they are often more complicated. Take for example the discussion about end-to-end encryption in WhatsApp. Governments and security agencies have argued that they need to be able to access such encrypted communication for security reasons, e.g. to be able to early detect possible terrorist attacks. Opponents of such access by the police and security agencies do

not only point at privacy considerations, but also at the fact that encrypted communication that cannot be accessed by governments and their agencies might be important for the democratic process, and that it enables opposition movements in countries with totalitarian or suppressive regimes.

A similar issue has arisen in relation to the Tor network. "Tor is free software and an open network that helps in defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy (Tor project 2017)." The networks operate as "a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet (Tor project 2017)." In the aftermath of the hacking of the Democratic Party during the US elections, it turned out that a Dutch private Tor server had probably been used in the hacking (Zenger 2017). The Tor server was owned by Rejo Zenger, A Dutch Bits of Freedom employee. Bits of Freedom describes itself as "the leading Dutch digital rights organization, focusing on privacy and communications freedom in the digital age (Bits of Freedom 2017)". While Zenger recognized that Tor servers can be misused by hackers, and are in that sense a threat to cybersecurity, he believes that this is a price worth paying, not only for reasons of privacy but also because these servers may be crucial for whistle blowers to reveal abuses. Again, the value that is at stake here is not just privacy but also a range of civil liberties that are seen as crucial for democracy and the democratic process.

Another example is profiling. In this case, values like non-discrimination and absence of bias are at stake and are potentially conflicting with security. In profiling, people are approached, judged or treated in a certain way because these have characteristics that fit a certain profile and that are associated with certain other traits (i.e. traits other than by which they are identified as belonging to the profile). Profiling is used for a wide range of purposes. It may be used by the police or security agencies to find criminals or terrorists; by airports to decide who to check more carefully, by (internet) companies to target certain consumers, by banks in deciding who to give a loan (and against what percentage). As these examples already suggest sometimes profiling serves security objectives. At the same time, profiling may inflict all kinds of undeserved harm on people, from nuisance to false accusations to even, in extreme cases, imprisonment of innocent people. Although profiling may involve privacy violations, because personal information is gathered to fit somebody into a profile, the main issue at stake is not privacy. Rather the issue is that a generalization is made based on limited information about a person. This generalization is based on statistical information about a group to which a person belongs while, due to its probabilistic nature, this information may say nothing about that particular person.

Profiling may lead to stereotyping and discrimination. For example, the use of facial recognition technologies by the police and security officers has led to such concerns. Some studies suggest that facial recognition cognition algorithms are less accurate for certain social groups or races, which may lead to racial bias in their use.

Another value issue that might arise due to the collection of data by certain organizations for security reasons and that is not completely covered by privacy is the creation of power imbalances. Economic monopolies or oligarchies are often considered undesirable, and in democracies, balancing the (political) power between citizens and their government is an important concern. Maintaining certain power balances is therefore considered important by many for a healthy economy and for democratic politics. What seems to be less recognized is that in the information age, the possession of information about others and their behavior is increasingly a source of power.

This also means that organizations that collect or possess large amounts of (personal) data may have increasingly power over other actors, which may lead to the disruption of existing power balances and the creation of new power imbalances. This applies to companies like Google or Facebook that collect large amounts of data about users and consumers, but also to governments and security agencies that may collect large amounts of data about citizens—and to providers of cybersecurity technologies as well, as they activities may involve the access to highly sensitive data. It should be noted that the accumulation of large amounts of data in the hands of a few may lead to new power imbalances and may be problematic even if such data is anonymized, or if people have given their informed consent for the collection, storage and use of their data. This means that even if privacy concerns are properly addressed, the accumulation of large amounts of data in the hands of a few may be considered problematic for economic as well as political reasons.

1.3 CYBER WARFARE:

Cyber-crime is typically understood to consist of accessing a computer without the owner's permission, exceeding the scope of one's approval to access a computer system, modifying or destroying computer data or using computer time and resources without proper authorization. Cyber-terrorism consists essentially of undertaking these same activities to advance one's political or ideological ends. This addresses this ethical issue of cyber warfare in the national security context. Terrorism and the Internet were highlighted in two main ways. First, the Internet has become a forum for terrorist groups and individual terrorists, both to spread their messages of hate and violence, as well as to communicate with one another and their sympathizers. Second, individuals and groups have tried to attack

computer networks, including those on the Internet. This second issue is described as cyber terrorism or cyber warfare. Phahlamohlaka argues that the security risks associated with information and communication technologies, which go beyond national boundaries, are not fully in line with the value of data protection of all states. She sees a need of developing and implementing agile security related ICT policies to mitigate the value conflict between data protection and security in the national security do-main to avoid cyber warfare. Building on this value conflict, Deibert discusses the growing pressure on governments to develop capacities to fight cyber wars. He notes that "today's deteriorating cyber-environment poses immediate threats to the maintenance of online freedom and longer-term threats to the integrity of global communications networks". His study highlights the value conflict between the data protection and security due to cyber wars.

Security of Critical National Infrastructure: The importance of critical national infrastructure protection was discussed in this chapter. To protect critical information assets, enable safe communications, and conduct effective military operations in cyberspace, an increasing pressing issue for the government is to compel adversaries to stop conducting intrusions that already have been highly successful, rather than deterring them from choosing to conduct new hostile intrusions in cyberspace. This requires a significant control in the cloud against hostile intrusions in order to achieve security.

State Security vs. Individual Security: This ethical issue is discussed in this chapter. Dunn Cavelty (2014) discusses a lack of focus on humans in the efforts of states to achieve security in the building of ICT and other critical infrastructures. As a result, he argues, state security is not aligned with individual security. In fact, the focus on state's security crowds out consideration for security of individuals resulting in detrimental effect of the whole system which allows the state actors to militarize cyber-security and to override the different security needs of individual humans in the cyberspace.

Cyber-Espionage: Cyber espionage is the use of electronic capabilities to illegally gather information from a target. This ethical issue was mentioned in this chapter. For all nations, the information technology revolution quietly changed the way governments operate. The asymmetrical threat posed by cyber attacks and the inherent vulnerabilities of cyberspace constitute a serious security risk confronting all nations. The achievements of cyber espionage - to which law enforcement and counterintelligence have found little answer - hint that more serious cyber-attacks on critical infrastructures are only a matter of time. Still, national security planners should address all threats with method and objectivity. As dependence on IT and the Internet grows, governments should make proportional

investments in network security, incident response to the cyber espionages, and manage technical training.

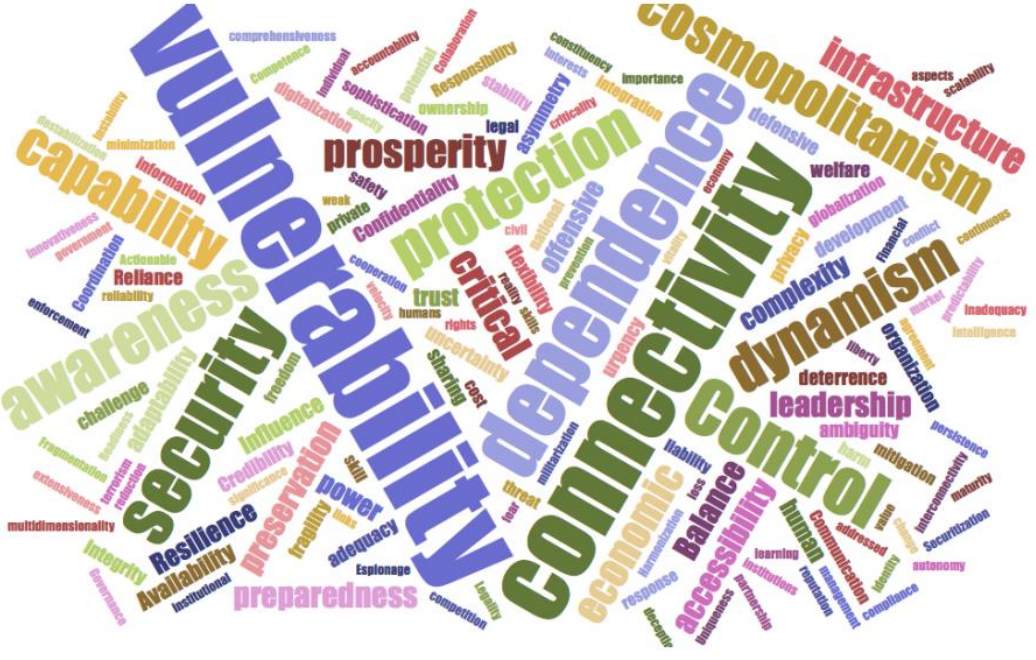
Data Breach: The release of data to an untrusted environment could lead to another crucial issue called data breach that is mentioned in this chapter. The recent massive critical data leaks by Wikileaks suggest how fragile national security is from the perspective of data breach. In the absence of strong cybersecurity in the national security domain, there is apparently a major value conflict between connectivity and security. This value conflict is highlighted in the existence of technology progress where technology was considered as a key contributor in the progress of any country, but also has created severe problems in the form of cyber security. Data breach raises several concerns. Firstly, critical infrastructure such as military and diplomatic systems may be vulnerable to security breaches. Secondly, such leak causes far-reaching damage to public interests, national security and economic sustainability. And thirdly, both technology and law seem incapable of dealing with such situation.

Lack of Cyber Law: The literature review reveals that legality problems play an important role in cybersecurity in the national security domain. The lack of cyber law is mentioned in this chapter. Lawyers are faced with insufficient and vague cybersecurity legislations, which are incompatible with the requirements for effectively dealing with cyber-crimes. At the same time, cyber laws become much critical than before in data and information security, as one can see in the growth of cyber-criminal activities. Government defined that digital crimes (e-crimes) impose new challenges on prevention, detection, investigation, and prosecution of the corresponding offences". Widely accessible systems must be made in a way that one can detect and investigate digital crimes more efficiently and effectively.

Surveillance: The ethical issue of monitoring of computer activities and data on the cyberspace by police and national security authorities is discussed in this paper. When considering different ethical issues regarding cybersecurity and national security, another major conflict set becomes apparent, i.e. the conflict between privacy and security. A critical issue in cyberspace lies in the inability of companies and private businesses to exchange information with the government. This causes insufficient information collection, skewing analyst results, and preventing the states from collecting sufficient data on cyber attacks and developing better defenses. The Google cyber-attacks illustrate the vulnerability of information stored in the cloud, online surveillance, and private sector collaboration with government agencies to prevent the increasing potential for catastrophic loss and global terrorism. Hiller and Russell state this fact again and argue that cyber infrastructure is owned and operated mainly by private rather than public entities; the states

therefore should select the most effective cybersecurity strategy and regulate the private sector in order to reduce overall cybersecurity risk and address privacy concerns on cyberspace.

The word cloud for national security looks different because the researcher identified a greater number of "thick" (descriptive and practical) values. This domain seems to avoid appealing to abstract principles (such as those of bioethics) and ethical-theory terms. It is rather oriented towards valuing a larger number of more practical, concrete desiderata at the political and organizational level.



This chapter emphasizes the multiplicity of relevant values in relation to cyber security in the national security domain. Much of the chapter in our book views cybersecurity as a necessary complement to national security strategies. National cybersecurity strategies need to be mindful of national cultures and ethical and technical values, yet compatible with international strategies and the global nature of the Internet.

Some chapters recognize the need to respect ethical and moral values such as security, freedom of expression, privacy protection and the free flow of information. In addition, other chapter stress the rule of law and accountability as key values. Several chapters explicitly state that cybersecurity became the top priority in dealing with the terrorism. In the following, we provide a more specific description on how the values are understood in the national security domain. We provide pairs of values that are usually coupled, which is denoted by "↔":

Accessibility ↔ Security: These two values play an important role in national security domain. With lower costs associated with information accessibility and retrieval, higher consumer and producer accessibility to global markets and transnational communication are achieved. Many internet users, however, are not fully aware of cyber threats and they are not trained to protect themselves against these threats, leaving them vulnerable to online exploits, so increasing insecurity in cyberspace.

Legality ↔ Safety/Security: A value often associated with safety and security in the national security domain is legality. This value refers to the effectiveness of laws in assisting the police and the juridical system in combating cyber-crimes and computer-related crimes. While it is possible to protect information resources and communication networks against criminal assault with cryptography; legal mechanisms should are needed to secure systems and deal with cyber-crimes

Privacy/Protection of Data ↔ Security: A lack of focus on humans from states in the efforts of achieving security in the building of ICT and other critical infrastructures causes a tension between individual and state security. In addition, counter-terrorism measures and tools that tackle cyber-crime often invade privacy in the most brutal ways and, at the same time, lack of personal online security leads to breaches of that same privacy. Security is thus an essential part of enabling privacy in the national security domain. That contains data security; data protection; data ownership; access control, information and computer security.

Confidentiality ↔ Trust: Confidentiality prevents the disclosure of information to unauthorized individuals or systems; Network information will not be leaked to unauthorized users or entity institutions. The impact of cyber-threats could reduce public confidence, damaging reputation of internet transactions. Thus, assuring a trusted and resilient information and communications infrastructure is needed. A reliable, resilient, trustworthy digital infrastructure for the future enhance online choice, efficiency, security and privacy.

Connectedness ↔ Equity of Access: Globally interconnected digital information and communications underpins almost every facet of modern society and provides critical infrastructure. Based on the literature review, inclusion and equity of access, consumer and producer accessibility to global markets, transnational communication, learning, and entertainment should be guaranteed along connectedness.

Accessibility ↔ Prosperity: Internet usage increases productivity, as a platform for innovation, and as a venue for new businesses; The value of accessibility therefore is an asset and an economic necessity. Since the private and public bodies offer more services online over time, once cyber-threats are addressed and systems are secured, the value of accessibility supports the value of prosperity accordingly.

Interconnectivity ↔ Security: The urgency for nations to develop strategies, frameworks or suitable legal policies to defend and protect from cyber-attacks were discussed in this chapter. At the same time, it is often mentioned that cyber-attacks are beyond borders. It is becoming increasingly difficult and complex to handle cyber-attacks counter measures. In fact, whereas interconnectivity boosts economic growth and makes people's life easier, it also gives potential attackers more opportunities to commit crimes.

Cyber Awareness ↔ Security: Raising awareness about cyber-security threats and vulnerabilities and their impact on society has become vital, but seem to be missing in the society, comparing to the leadership that the governments of nations try to establish. Through awareness-raising, individual and corporate users can learn how to behave in the online world and protect themselves from typical risks. Awareness activities occur on an ongoing basis and use a variety of delivery methods to reach broad audiences. The awareness-raising, however, varies across countries. Security awareness activities may be triggered by different events or factors, which may be internal or external to an organisation. Major external factors could include: recent security breaches, threats and incidents, new risks, updates of security policy and/or strategy.

1.4 OBSERVATIONS IN CYBER ETHICS:

A first observation is that the ethics of cybersecurity not an established subject, academically or in any other domain of operation. It is actually a rather under-developed topic within ICT ethics, where the majority of published work discusses issues such as "big data" and privacy or ethical issues of surveillance. In those cases, cybersecurity is usually only instrumentally discussed as a tool to protect (or undermine) privacy.

A second observation is that there are both common theme and differences across the three domains examined. In all domains, cybersecurity is recognized as being an instrumental value, not an end in itself, which opens up the possibility of trade-offs with different values in different spheres. The most prominent common theme is perhaps the existence of trade-offs and even conflicts between reasonable goals, for example between usability and security, accessibility and security, privacy and convenience. Other prominent common themes are the importance of cybersecurity to sustain trust (in institutions), and the harmful effect of any loss of control over data. The most prominent difference across the three domains regards the value of privacy, that is emphasized in business and health (together with confidentiality), but not in the national security domain, which appears concerned, above all, with the protecting the security and connectivity of infrastructure.

A third observation is that the ethical issues and dilemmas that the technological experts face in their daily life are to an insufficient degree represented in the literature, which may have several reasons, among which may be a lack of technical expertise of technology ethicists and a culture of secrecy among cybersecurity experts.

Finally, it is noteworthy that cybersecurity has different connotations in different social domains and these connotations affect the framing of problems and value assumptions in each domain. It is therefore plausible to think that thematic cross-pollution across different disciplines could be particularly fruitful. The health-related discussion could benefit from a little more emphasis on the need to protect vulnerable infrastructure. The discussion in national security could benefit from taking privacy more seriously. The discussion in business could also benefit from considering cybersecurity as a public good, to which businesses ought to contribute, rather than as (very important) factor in the relationship with its customer.

CHAPTER 2

PRINCIPLES IN CYBERSECURITY

2.1 CYBERSECURITY ESSENTIALS:

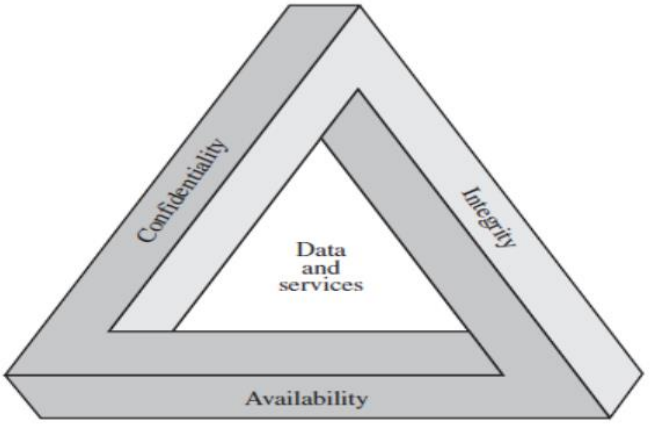
Cyber Security is a very complex term which passes through multi-dimensional request and response. In the current age, it is a challenging task for a small enterprise to big enterprise to secure themselves from external and internal cyber-attacks. Cyber Security is a subset of information security which deals with securing the information, data and from both internal and external cyber threats. It is a proactive practice to safeguard the confidential information of the organization from unauthorized access by enforcing the layered security policies and protocol. The task is more complex due to the variety of nature of cyber-attacks and the inability of quality response in the absence of adequate security measures.

The word 'Cyber' is not singular; it has its many forms to understand the concept using different terminologies such as:

A. Cyber Space: It's a virtual world of the digital data formed by bits.

B. Cyber Economy: Complex structure of interconnected networked systems and its environment. Cyber Space is a manmade ecosystem. It comprises of all interconnected networks, database, a source of information.

Cyber Space is not only including the software, hardware, data and information system, but the people surrounding it and social interaction within this network and infrastructure. According to NIST (National Institute of Standards and Technology), Cyber Security is "The ability to protect or defend the use of cyberspace from cyber attacks."



Information content & information determinacy determine the type of software applications. Content refers to input & output data, determinacy refers to the predictability of order & timing of information There are three different tools which are useful for system designers to make a robust and secure product i.e. Confidentiality, Integrity, and Availability.

In the above image, there are three key concepts shown and all three are related to each other, which is known as the CIA triad, it is considered to be the main pillars of the security, which anyone who protects an information system must understand: Confidentiality, Integrity, and Availability. Each component is critical to overall security, with the failure of any one component resulting in potential system compromise.

Confidentiality: It means to protect personal privacy information from unauthorized access to devices, processes or individuals. If we understand it in the parts, it can be described as Information must have protection enable from the different types of users to access it. There must be a limitation to access the information, who are authorized can only access the information. And last the authentication system which authenticates the user before accessing information.

Integrity: It normally refers to the data integrity, or to make ensure that data stored is accurate and no unauthorized modifications are done. The loss of integrity is considered as the unauthorized modification or destruction of the information. Disrupting a message in transit can have serious consequences. For E.g.: if it is possible to modify the fund transfer message during online banking, an attacker can take this advantage to fulfill his or

her benefit by stealing the credentials. So to ensure the integrity of this type of message is important for any security systems.

Availability: Ensuring the timely and reliable access of information to the authorized users for the systems to provide a value. The loss of the availability of the information is the loss or disruption of access to the information. Although the use of CIA TRIAD to define security objective is well established, there are additional concepts which are important to learn and understand which makes the complete picture, they are Authentication, Authorization, and Nonrepudiation. Understanding each of the six concepts will help to implement robust security mechanisms.

Authentication: The primary goal is to focus the information on being genuine and source of the message for any security systems. This means that users are who they say and every piece of information came from the trusted source. Nowadays we have seen Authentication system requires more than one factor of authentication, it is called Multifactor Authentication. Such as password required combining with Fingerprint or retina scan or voice verification and PIN (Personal Identification Number), as it is useful in validating the user (owner of the fingerprint) and PIN number (something that user knows).

Authorization: It focuses on whether the user is verifiably granted permission to do so. When the system authenticates the user it also verifies and checks access privileges granted to the user. Which in simple terms means what a user can or cannot do while using the system.

Nonrepudiation: It is assuring that the sender of the data is provided with the proof of delivery and recipient is provided with the sender's identity, so neither can deny in later part of having processed the data. In the normal physical world, it can be understood as the notary done on the stamp paper for any kind of deals. Where neither of the parties can deny the deal in the later stages. To meet such requirements, systems have to normally rely on the asymmetric cryptography or public key cryptography. While symmetric key systems use a single key to encrypt and decrypt the data. Asymmetric cryptography uses one key(private) for signing the data and another key(public) for verifying the data.

Cryptography: A cryptographic algorithm is a mathematical function which is used in encryption and decryption process. While cryptography is a science of securing data, cryptanalysis is the science of analyzing and breaking secure communication without knowledge of the key. Combining both Cryptography + Cryptanalysis = Cryptology The most common to known is the classical cipher is the substitution cipher which works by

substituting each letter in the alphabet with one another when writing the secret message. The key here is the number of characters which is used for substitution.

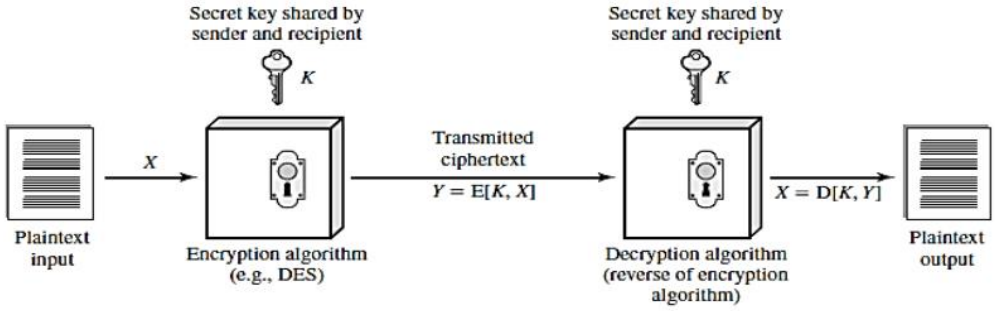
Below is one such example:

abcdefghijklmnopqrstuvwxyz

nopqrstuvwxyzabcdefghijklm

where a=n, b=o, c=p, d=q and so on Using this cipher, the message, "hello world" would be written as "uryybjbeyq". It is a simple substitution cipher known as Caeser Cipher.

Symmetric Encryption: Symmetric Encryption is also known as conventional encryption which has been introduced in the late 1970s. This technique is used to provide confidentiality for the data transmission or to store data using the symmetric encryption method. There are two well-known symmetric encryption algorithms used they are: Data Encryption Standard(DES) and Advanced Encryption Standard (AES), both algorithms are block cipher encryption algorithms



Plaintext: Original message or data provided as input into the algorithm.

Encryption Algorithm: Encryption algorithm used which performs operations on the plaintext.

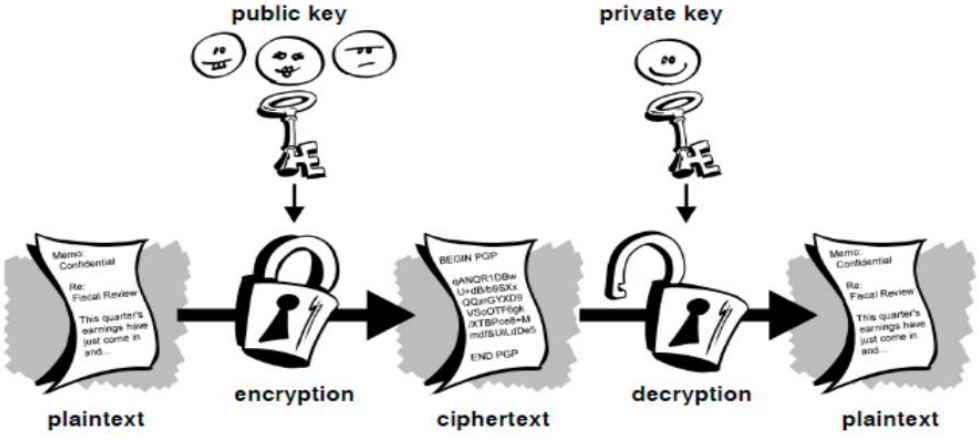
Secret Key: Secret Key is also an input provided to the encryption algorithm. The exact number of substitution or transformations performed by an algorithm depending on the key.

Cipher text: Encrypted message which is produced as output which depends on the plaintext and key used. For the same message, if there are different keys used, cipher text will be different for both keys used.

Decryption Algorithm: It is the same encryption algorithm which runs in the reverse manner which takes the cipher text and secret key as the input and generates the original plaintext. There are two requirements for the symmetric encryption algorithms to work, the first one is strong encryption algorithms know to both the party sender and receiver and the second one is the secret key should be known only to sender and receiver only.

Ceaser cipher is a very form of symmetric key encryption. Symmetric cryptography doesn't address the following issue: Attacker can eavesdrop the shared key between sender and receiver and can steal the key and decrypt the data. This is where the concept of the Public Key Encryption OR Asymmetric key cryptography comes in picture.

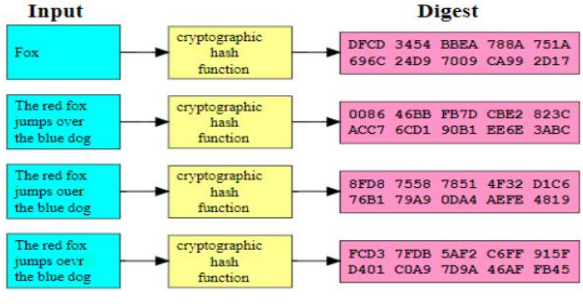
Asymmetric encryption: Asymmetric encryption is also known as Public Key key cryptography. It uses two mathematically related but unique keys: a public key and a private key. Each key has its own unique function. The public key is used to encrypt the data and the private key is used to decrypt the data. It is computationally infeasible to obtain the private key from the public key. Its primarily used for the authentication, non-repudiation and key exchange. Anyone with the public key can encrypt the data but cannot decrypt the same. Only the appropriate receiver with the private key can decrypt the data. Even if the attacker knows that the sender is transmitting data to the receiver, also data passes through multiple channels, there is nothing he or she can do. As the data can only be decrypted by the private key.



All communication which takes part between sender and receiver includes the public key. The private key is never shared; they are simply stored on the software or on the machine used. Some of the examples of the public key cryptosystem are Elgamal (named after its inventor TaherElgamal), RSA (Ron Rivest, Adi Shamir, Leonard Adleman) which is most widely used even in current times. Diffie-Hellman.

Hash Functions:

Cryptographic Hash Functions are a mathematical algorithm that take the input of the arbitrary size of data and generates the fixed length hash value or message digest or simply digest and they are also designed to be the one-way functions. This means they are not reversible in nature. There are few properties of the HASH Function which are mentioned below due to which they are still widely used in a different information security application.



• It is deterministic which means it will always give the same hash value for the same input message.

• Computing hash value of the message is faster.

• It is infeasible to generate the same message from the hash value.

• Even a very small change in the message will change the hash value completely.

• It is infeasible to find two different messages with the same hash value. Due to such properties they are widely used for digital signatures, Message Authentication Code, Indexing data in the hash table, fingerprinting, finding duplicate data, Checksums to identify any modification in data. Hash Algorithms which are commonly used today:

• Message Digest (MD) Algorithm: A byte-oriented algorithms that produce a 128-bit hash value from an arbitrary-length message. There are various versions of these algorithms present such as MD2(RFC 1319), MD4(RFC 1320), MD5(RFC 1321). MD5 is the third message digest algorithm after MD3 and MD4, which process data in 512-bit blocks which is broke down into 16 words composed of 32 bit each. The output from MD5 is 128-bit message digest value.

• Secure Hash Algorithm: It is a cryptographic hash function published by the National Institute of Standards and Technology (NIST) as a U.S. Federal Information Processing Standard which takes an input and produces a 160-bit hash value known as a message digest – typically rendered as a hexadecimal number which is 40 digits long. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions. There are a series of algorithms exist such as SHA-1, SHA-2, SHA-3. Apart from this, there are other well-known HASH Functions exist which are used such as RIPEMD, WhirlPool.

Digital Certificate: There are several issues which exist with the public key cryptosystems; one of them is the man-in-the-middle attack in which is one of the potential threat. In this attack someone tries to fake the key with user ID and name, and tried to pretend the same person, which is not and resulting in this, the data is encrypted with the attackers key. It is vital to know that the public key to which you are encrypting the data is the actual key of the intended recipient and not a forged one.

To overcome this, Digital Certificates has been introduced, which will ensure that whether a public key truly belongs to the actual owner or not. It acts much like a physical certificate. Digital certificates consist of three things:

- A Public Key.

- Certificate Information (Identity information about the user).

- One or more digital signature

Public key infrastructure: A Public Key Infrastructure (PKI) is a combination of policies, role, and procedures, which are needed to create, manage, distribute, use, store, and revoke digital certificates and manage, public-key encryption. It includes components such as Certificate Authority (CA) and the Registration Authority (RA). Certificate Authority creates a certificate and digitally signs them using its own private key. As it is the central component of the PKI system. Using the public key of the CA one can verify the authenticity of the digital certificate and can check the integrity of the content of the certificate. Registration Authority refers to the people which can include group, company, process, and tools which will help users to enroll them with the PKI system. It also checks the public key belongs to its owner or not. On the other hand, CA is the software which issues the actual certificates.

2.2 THREAT AND VULNERABILITIES OF CYBER SECURITY:

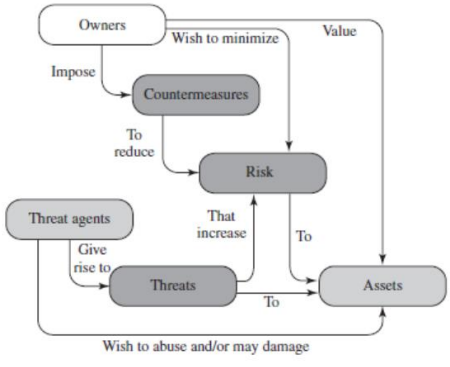
Attack Vector: An attack vector is defined as the technique by which unauthorized access is gained inside the computer or network for a criminal purpose by exploiting the vulnerabilities in the system.

Risk: It can be defined as the probability of the loss from any particular threat from the threat landscape, which can exploit the system and gain the benefits from it such as loss of private and confidential information such as username and password, sensitive organization data, also the loss of the reputation which has occurred can be considered. Also, the loss occurred in terms of damage or destruction of hardware and software assets can be considered as Risk.

Threat: Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset

Vulnerability: Weaknesses or gaps in a systems security program, design policies and implementation that can be exploited by different threats to gain unauthorized access of a computer system or network

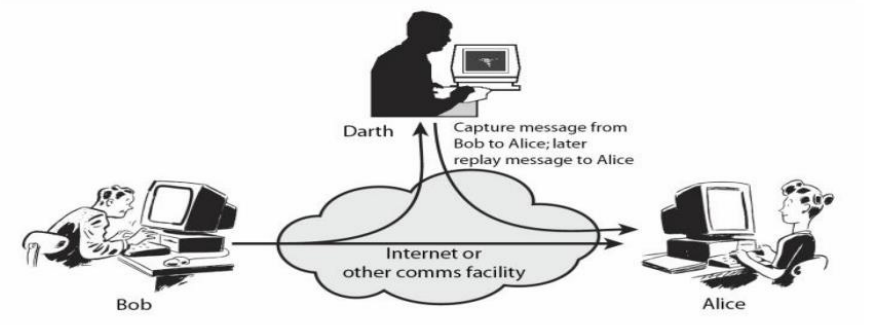
Asset: People, property, and information. People may include employees and customers. Property assets consist of both tangible and intangible items that can be assigned a value. Intangible assets include reputation and proprietary information. Information may include databases, software code, critical company records, and many other intangible items.



Counter Measure: An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, or by minimizing the harm it can cause, or by discovering and reporting it so that corrective and proactive action can be taken

Attack in Cyber security: We have already seen the definition of the attack on the previous page, we will look here the subtypes of attack and they are Active Attacks and Passive Attacks

Active Attacks: In an active attack, the attacker intercepts the connection and then modifies information.



An active attack can be divided further into Masquerade, Replay attack, Modification of messages.

Inside Attack: If the origin of the threat agent is from the inside the organization, which may have the authorization and access granted to the resources, but uses it with the criminal intent.

Outside Attack: Origin or source of the attack is from the outside of the organization and gains the unauthorized access to the system or resources with the criminal intent.

A Cyber attack can destroy the business overnight; a proper security defense is required to stop such attacks. The main focus is to compromise the systems and gain access to sensitive data. Let us see the top cyber security attack and what do they do.

Phishing Attack: It is a type of security attack that tricks the user to divulge the sensitive and personal/confidential information which is sometimes referred to as "Phishing Scam" also. Definitely, every user will not click the links provided in the email id for providing the details, but the attackers are smart they will perform the social engineering and will send the emails to the users with the similar content which user is already looking or interested in it.

The most targeted business sectors are Payment Platforms, Financial and Banking organizations, Webmail services and Cloud storage/hosting providers. Phishing attacks engage users with a specific message and very solicit way for the response from the user which is ideally to click on the link is known as "Call To Action". Which means the attacker wants the user action on the link provided in the email to perform the action.

Spear phishing: When a phishing attack is targeted to the specific individuals of the organization, it is known as spear phishing. Attackers use the solicit company logo, footer and all other style information which is present in the legit email to trick the user. The content of the email mainly focuses on the password reset email or, account reset activity. For the prevention of the phishing, the user has to check clearly the from address and email content, along with the links present in the email body. Apart from this, employees awareness using various teaching method is the most important as major data breach occurs due to human error which cannot be ignored.

SQL Injection Attack: SQL which is pronounced as "squeal" stands for the structured query language. It's a programming language used to communicate with databases. It is used to store critical data of websites/users/services in their databases which can contain personal and sensitive information such as username and password, transaction details.

SQL Injection attack targets the database using specifically crafted SQL statements to trick the system into unexpected and undesired outputs. SQL Injection attack can be carried out in different ways which can be decided after the attacker identifies system behavior.

If the web application is building a SQL query string dynamically with the account number the user will provide, it might look something like this

: "SELECT * FROM customers WHERE account = '" +userProvidedAccountNumber +"';"

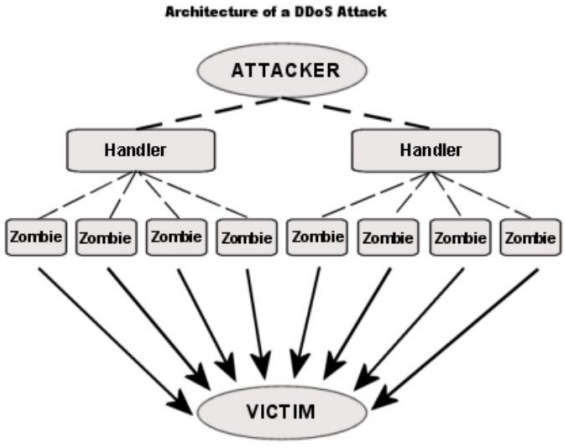
While this works for users who are properly entering their account number, it leaves the door open for attackers.

For example, if someone decided to provide an account number of "' or '1' = '1", that would result in a query string of:

"SELECT * FROM customers WHERE account = '' or '1' = '1';"

Due to the '1' = '1' always evaluates to TRUE, sending this statement to the database will result in the data for all customers being returned instead of just a single customer. The above query might not work for all the database, but it can work where there are less or no security measures taken to filter such SQL injection queries. Other types of SQL injection attacks include Blind SQL Injection, Out of Bound SQL Injection. SQL Injection attack can be prevented by avoiding the use of dynamic SQL, sanitize user inputs, don't

store data in plaintext, provide access control and privileges also use of web application firewall is also must.



Denial-of-service(DOS) and Distributed Denial of Service(DDOS): Denial-of-Service attack focus on disrupting or preventing legitimate users from accessing the websites or application or any other resources by sending flood of messages, packets, & connection requests, causing the target to slow down or "crash", rendering it unavailable to its users. Attacker mostly targets high-end value organizations such as media houses, banking, and financial organization, E-Commerce to disrupt their services. When the majority of present-day DoS attacks involve a number of systems (even into the hundreds of thousands) under the attacker's control which are installed with the bots, all simultaneously attacking the target. This coordination of attacking systems is referred to as a "Distributed Denial-of-Service" (DDoS).

Man-In-The-Middle Attack and Session Hijacking: Man-in-the-middle attacks are a common type of cyber security attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation they should normally not be able to listen. When a user is using the internet and our computer performs a lot back and forth transaction, the application generates and uses a session ID which will be unique and to make the transactions private between user and application. The attacker hijacks the session ID to eavesdrop the communication between user and application. There are various types of Man-In-The-Middle Attack such as Rogue access points, ARP Spoofing, DNS Spoofing, Packet Injection, SSL Striping. We can prevent such attacks by

using strong WEP/WAP encryption on access points, using a virtual private network (VPN), enforce https and using a strong combination of the public key pair authentication.

Brute-Force Attack(Password Attack): The theory behind such an attack is that if you take an infinite number of attempts to guess a password, you are bound to be right eventually. The term brute-force means overpowering the system through repetition. A brute force attack is among the simplest and least sophisticated hacking method. Brute Force attacks often use automated systems or tools to perform the attack in which different password combinations are used to try to gain entry to a network, such as a dictionary attack list or using rainbow tables. The attacker aims to forcefully gain access to a user account by attempting to guess the username/email and password.

Usually, the motive behind it is to use the breached account to execute a large-scale attack, steal sensitive data, shut down the system, or a combination of the three. We can prevent it by using a strong password combination policy and require to change a password on regular intervals, locking out accounts on a certain number of incorrect password attempts, use captcha, two-factor authentication, monitoring server logs, limit logins from the single IP/Range.

Malware Attack: Malware can be described as Malicious software that is installed in your system without your consent. It can attach itself to the legitimate process or replicate itself or can put itself to startup. The objective of the malware could be to exfiltrate information, disrupt business operations, demand payment, There are many types of malware below are some of the commonly known types:

Macro Virus: These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

Trojans: A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers.

Logic bombs: A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.

Worms: Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm can result in denial-of-service attacks against nodes on the network.

Dropper: A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.

Ransomware: Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion and asks for the payment in bitcoin Which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key or using the decryptor if it is available.

Adware: Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.

Spyware: Spyware is a type of program that is installed to collect information about users, their computers or their browsing history. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

Zero-Day Exploit: A zero-day exploit hits after a vulnerability has been announced, but before a patch or solution is implemented. Attacker targets the disclosed vulnerability during this window of time.

To prevent such attack we need to ensure that the anti-virus product is up-to-date with the latest signatures, continues user education, performing regular audits, regular backup of the websites, application, and databases at multiple locations. Now we will start with

understanding the complete Risk Rating Methodology. It will also include different steps such as Risk Analysis, Risk Assessment, and Risk Management.

2.3 RISK ASSESSMENT IN CYBER SECURITY:

Identifying threats and vulnerabilities is very important to build a robust security architecture. It always starts with identifying what are the important assets which need to be secured from threats. So the first and foremost task is to define the scope of the cybersecurity Risk Assessment. Being able to estimate the associated risk to the business is very important.

$$\text{Risk} = \frac{\text{Assets} * \text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures (controls)}}$$

- Assets – what we are trying to protect
- Threats – what we are trying to protect against
- Vulnerability – what we are trying to address
- Controls – what we are doing to address them

Assets: We have seen the definition of the Assets in the first section under key terminologies. Now we will understand the assets in relation to threat actions and will map with the CIA triad. Assets can be categorized in various types such as hardware, software, Data, and communication channel (different devices including communication cables). In details if we go it can be described as follow:

Physical assets such as Computer, Laptop, Networking Devices, Storage Devices, etc. Software such as Operating system, Application Running on the system, services running, port scanning, API services, protocols used, and policies. All this can be considered as an important asset and are part of the scope of the Risk Assessment. One may identify security

concerns in architecture or design. By using this process it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time when there is a situation arise to take the critical business decision to reduce the impact.

Asset Value Assessment: This would be the first involved in measuring the asset value which is part of the critical business process. An asset can be the people, process, hardware, software, data, any tangible or intangible (can include the reputation of the organization, loss of customer and services) things which are part of the critical business process. In order to achieve greater control in risk and with effective least cost, identifying and prioritizing the assets are a critical part of the process from top priority to least priority. This can be achieved by identifying the core functions and the process of the organization. Along with this identifying the physical infrastructure, assets which can be critical hardware or software related to the business functions and safety measures which are preinstalled for the emergency situations need to be also considered.

Threats actions and its Consequences: we will see some terminologies related to the threat, we have already seen the definition of the threat in the first section of key terminologies. After identifying the asset value assessment and quantifying it, next step is to conduct the Threat assessment where the potential threats are identified. There is another relative term "Hazard" is also used for the threats which are natural or not man-made, such as earthquake, flood or wind disaster which also needs to be considered and the man-made hazard can be either technological threats or terrorism which we can refer as "Threats" for simplicity.

• Threat Action: It is an assault on system security.

• Threat Analysis: An analysis of the probability of occurrences and consequences of damaging actions to a system.

• Threat Consequence: A security violation that results from a threat action. Includes disclosure, deception, disruption, and usurpation.

Threat Analysis: Our next goal here is to estimate the likelihood of a successful attack by this group of threat agents for this we will use the OWASP risk rating methodology for preparing severity of the Risk Assessment Model.

Skill level: How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9),

Motive: How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

Opportunity: What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

Size: How large is this group of threat agents? Developers (2), system admins (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

The use of a rating system will help in the quantification of risk. There is always difficulty in justifying the protection of assets. Management is better able to understand the implications of the threat and vulnerabilities when they are presented in the form of numbers and statistics which means quantifiable and measurable.

Vulnerability Analysis:

Vulnerability is a weakness that a threat can exploit to breach security and harm your organization. Vulnerabilities can be identified through vulnerability analysis, audit reports, the NIST vulnerability database, and vendor data. The problem faced within many organizations is the ability to effectively filter out the false positives from assessment applications. The result of the various manual and automated tools must be verified in order to accurately determine the reliability of the tools in use and to avoid protecting an area that in reality does not exist. False positive results can be mitigated by ensuring that the assessment applications are up to date with the latest stable signatures and patches. There are two ways penetration testing and vulnerability analysis can be done, one with having the knowledge of the systems and topology, another with zero knowledge which is mostly conducted externally known as black box testing.

Examples of vulnerabilities:

• Lack of sufficient logging mechanism

• Input validation vulnerability

• Sensitive data protection vulnerability

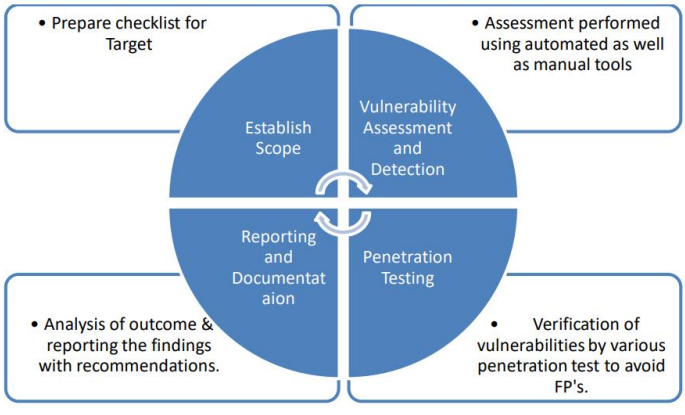
• Session management vulnerability

• Cryptographic vulnerability

• Memory leak Issue

• Cross-site request forgery

• Remote Code Execution



Vulnerability Factors: The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above

Ease of discovery: How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

Ease of exploit: How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

Awareness: How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

Intrusion detection: How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9).

Estimating Impact: When estimating the impact of the successful attack, it is important to consider the technical impact and business impact.

Ultimately the business impact would be more important. So by providing the appropriate technical risk details which will enable management to make the decision about the business risk.

Technical Impact Factors: The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

Loss of confidentiality: How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)

Loss of integrity: How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)

Loss of availability: How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)

Loss of accountability: Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9).

Business Impact Factors: Business impact requires a deep understanding of the different operations on which the company is working and gets maximum return on investment.

There are many factors and also may not be the same for all organization, but we will see some of the common impact factors.

A. Financial damage: How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)

B. Reputation damage: Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)

C.Non-compliance: How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)

D.Privacy violation: How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9).

The severity of RISK: We will now prepare the severity of the risk which can be obtained by combining the different impact factors. It is divided into three parts from a 0-9 scale, low medium or high as shown below.

Impact Scale	Impact Levels
0-<3	LOW
3-<6	MEDIUM
6-9	HIGH

Countermeasures (Control): In this step, we have to identify the existing security policies and protocols which are placed. Are they are adequate with the current threat landscape? Or it needs to modify and update the security posture of the organization. What level of risk is acceptable to the organization. This will help the security team and top management to understand the risk levels and they can focus on more high-level risks

Documentation: This is the final step in which risk assessment report is prepared to support the management to take appropriate decision on policies, procedures, budget allocation. For each threat, the report should have corresponding vulnerabilities, assets at risk, impact, and control remediation.

2.4 ADVANCE PERSISTENT THREAT AND CYBER KILL CHAIN:

In today's world organizations are facing critical issues from different types of advanced threats including to the traditional ones. However, they are still finding issues that how the Advanced Persistent Threat which is known as APT can be handled in a way those traditional threats are handled. Well, APT is much complex in nature that they cannot be handled with any single approach. It is not possible to secure any organization to handle entire security and APT in a single way. Organizations are dealing with the APT's they are completely different in nature until the organization understands where the real issue lies and how to solve them. To understand how to handle Advanced Persistent Threats first executives of the organization has to understand the motive behind the attack.

As still management of many organizations still thinks that they have paid or invested enough to handle every kind of cyber attack. Because spending the money will not solve the issue of complete security from Advanced Threats. In the current situations or in simple terms the traditional method which is followed is to install basic security mechanisms. Then they get compromised, they will get notifications from the law enforcement and then they start the forensic investigation. APT's are well funded, organized group of hackers who in a systematical manner to compromise the target which is mostly government organization's, private company's. They are mainly focused on gathering critical data by exploiting the vulnerability in a stealthy manner. They are very smart in hiding their tracks. They bypass highly secure infrastructure to establish the foot-hold in the target organization and to remain there until and unless the motive is not completed.

If we look deep into the APT, attacker needs one vulnerability to compromise the security and make way to get into the organization. But for the organization, they need to find out all vulnerability and to patch them. Many organization does not still understand that what are all the point of entry points or attack vectors from where the attacker can exploit it and make their way inside. The success ratio of APT is good, as they keep on trying until they find a way to exploit the system of the target. For APT we have to learn them first before we try to stop them. Instead of looking in the future we can start learning the APT now and we can try to build the defense based on the learning from the past attacks. Though we cannot be sure that there will be no new approach.

But there are chances that same cybercriminal groups tend to use similar tactics and techniques on similar organizations. The key objective should assume the worst attack ever and hope for the best. It will help to understand the security level of your organization and will learn something new, while indirectly help to improve the security posture of the

organization. Instead of assuming the best security measures are applied and doing nothing. The final goal should be, an organization should not lose the business due to the lack of cybersecurity measures and practice. Most of the organization so spend large amount behind the cybersecurity and defend them. But the fundamental point is to understand is to identify the priority and risk and returns from the investment. The reason behind failure to defend from APT is to identify what resources which are at high risk needs more protection.

There are multiple protection mechanisms which are already in place where the APT attack has been seen such as:

- Firewall
- Application Filtering
- End-Point Detection
- Anti-Virus Solutions
- Intrusion Detection

Investing a large amount of money to defend an organization from APT doesn't guarantee the protection from the APT. But the organization should focus on high-risk vulnerabilities and resources which can cause a big impact. It is better to fix 2 high-risk vulnerabilities which can cause a big impact instead of fixing low risk 20 vulnerabilities which cause not threats. Let us now start to learn more about the APT, what does it mean and how it works.

Advance Persistent Threat: The term APT sounds very simple but is often taken as for granted or been misunderstood. The term Advance is related to the systematically crafting an attack vector in terms of its advanced and very targeted code used which is very effective. The way attacker crafts the attack is very advanced while the methods to deliver the same are very standard methods and most important that it will work. Most of the APT will take advantage of the available advanced technology and techniques to customize the attack. In every APT there will be a single method which will be used to bypass the security devices, which is known as Encryption. It was created to stop attackers from accessing critical information. Most security devices are unable to read the encrypted code of payload or encrypted packets in the network. The attacker sets up the encrypted outbound tunnel to

attacker system. So data is encrypted and it goes undetected on the network. The next is persistent. The attacker will not stop after failing once or twice.

They will keep trying until they are successful in their objective. There need to be continuous defensive measured should be established. The persistent nature of an APT is what it causes more damage to the organization. It simply means to remain stealthy for a prolonged period of time and not get caught due to its state of the art coding techniques. They get into the system, remain there until the data is completely exfiltrated, and they leave without getting on the surface and they do not leave any trace. So it becomes very hard for an organization during the post-investigation when any third party services such as law enforcement agency inform them regarding the APT attack on your organization. It would be very difficult for an organization, as they don't know where to start an investigation and how to decide a timeline for that.

As mainly APT attacks are not for a few days, an attacker could have a foothold in systems from many days, weeks, months or sometimes it may be years. The persistent process suggests that an external command and control system is continuously monitoring and extracting data from a specific target. The "Threat" process indicates human involvement in orchestrating the attack. For an APT to work successfully, it' important to hide the identity of the attackers, as APT attribution could lead to some real-world conflicts. So the attackers will want to hide their tracks. It is not uncommon to see the use of unpatched vulnerabilities (zero-days) in this kind of operations.

APT will gather as much as information as possible so it will help the attacker to customize the attack to become successful.

APT Intentions: For a defender, it is very important to find out the intentions behind the APT attack. That would be useful in investigating the post-incident analysis. We will look into some of the intentions of the attacker which were concluded based on the previous APT attacks.

Data: For any organization, it is important to understand the market strategy, other competitive organization working in the similar product market. The intentions behind such type of attack in which an attacker tries to exfiltrate data such as proprietary designs, schematics, formulas, experiment details, source code.

Information: It is very important for any organization to keep internal information in a very closed loop. Such as its financial status, future Corporate directions, its mergers, and acquisitions. This type of information is very useful to target the organization.

APT Threat Vectors:

External:

Internet:

• Email Attachments

• File Sharing

• Pirated Software

• Mass vulnerability Exploits

Physical:

• Infection using external devices(USB, CD, External Disk Drives)

• Malicious IT Equipment

• Rogue Wifi Access points

• Stolen Mobile devices / Laptops

Internal:

Trusted Insider:

• Rogue Employee

• Third Party Contractors & Vendors Trusted Channel:

• Stolen Credentials

• P2P tapping

• Un-Trusted devices

• Hijacked Cell communications

There are other threat vectors which are also present which are related to Software used inside the organizations.

Insecure Build:

• Insecure Devices.

• Unpatched software versions.

• Misconfigured Device.

Information Leakage:

• Exposure of sensitive material on online/social media.

Application Security:

• Fuzzing / Reverse Engineering.

• Buffer Overflows

APT- Tools:

• Open Source exploit Softwares

• Malware: Botnets, Rootkits, Ransomware, Malicious Attachments

• Open source Available Exploit Code

• Using Zero Days.

APT- Techniques:

• Open Source Intelligence (OSINT)

Social Engineering / Using SET (Social Engineering Toolkit)

o Leverage Social media information.

o Identify contextual and behavioral information.

Spear Phishing Attack:

o Requires in-depth knowledge of internal communication method.

o Requires to build a strategy which lures the target and perform a predetermined action which.

Malicious Attachments:

o File format such as PDF, Office (Word/Excel/Access) is used mostly in APTs.

o Usage of exploit kits to generate the documents which contain malicious macros and craft the malicious attachments to send it the target using a properly crafted email.

Such as Fallout, Angler, RIG, Nuclear, Neutrino are well-known examples of exploit kits.

o Exploits are easy to use, can be easily obtained from the dark web.

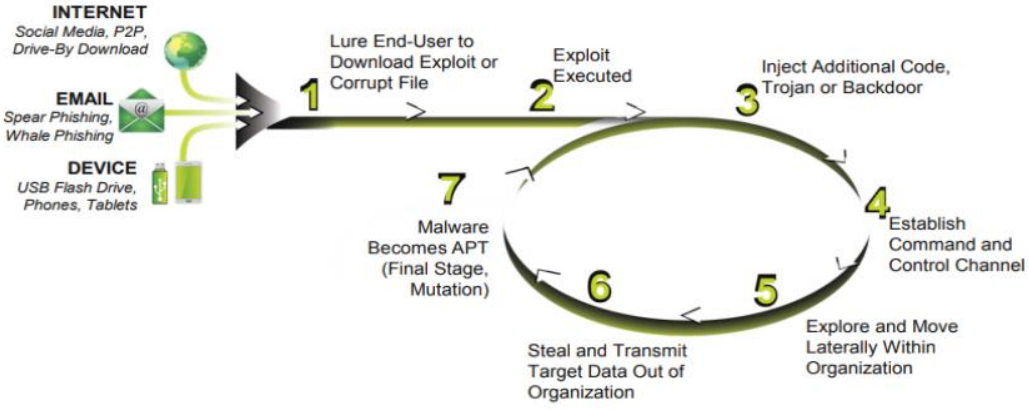
o Provides command and control infrastructure services

Hardware Devices:

o Hardware exploits in the internal devices used.

o Projectors, Printers, Shared file servers, which are now usually connected with the internet, they are left open which out any security measures. An attacker tries to use such resources gain access to the internal network.

In the below image, we can clearly see and understand how the different attack vectors take part in making a successful APT attack



Defending Against APT:

We will see some of the high-level strategies that an organization must use to defend against the APT. It is always important that prevention is good but detection is a must. Mostly, the organization builds and invest in preventive measures. But they forget that such type of APT attacks mostly comes with the legitimate traffic inside the organization and which is very difficult to identify by the installed security measures. There are few things which an organization must do to prevent against such threats.

Raise Awareness and Control Users: Humans which are considered the end user and are targeted mostly to perform malicious actions, though they are not known what will be the consequences when clicks on such unknown links in the email. So it is better to conduct

the internal phishing test and user awareness by giving basic ideas regarding phishing and how to identify them.

Reputation Scoring and Malicious Traffic Identification: Traditional security measures work on to block or access network traffic. While in APT mostly in pretends to the legitimate traffic. Once they enter into the network, they become bad or evil. So it is better to monitor the network traffic and scoring them based on their behavior in the network. That will help to identify if any malicious packets try to change its behavior from good to bad.

Monitor Outbound Traffic: Security Measures are generally built around the inbound traffic and monitor it to stop the threats from spreading. While in APTs, it is also important to monitor outbound traffic as their motive is to exfiltrate the internal data which will harm the organization. So it important to detect the anomaly in the outbound traffic also.

Understand the changing Threat Landscape: It is difficult when we don't know from what we have to defend to save ourselves. Something which is unknown or unseen. The only way to defend is to understand and learn how the offensive part works and operates. If the organization will not learn the new attack techniques and tactics they will lose the battle and not be able to tune their defensive measures.

Manage Endpoint: The ultimate goal of the attacker is to steal information which is stored on the endpoint. So even if the attacker has access inside the network, they still need to access the endpoint to get the information. So to limit the damage, controlling the endpoint and locking down endpoint by disconnecting it from other networks and isolating it will protect the information from getting outside of the organization.

Now we will learn the complete and in-depth process and stages which the attacker performed to conduct such an APT attack. It is very important to learn each kill stage components in detail. This complete cycle is known as the Cyber Kill Chain. It can simply be understood as a chain of multiple stages which are related to each other. The output of each stage can be considered as input for the next stage. We will see the offensive steps which are part of the cyber kill chain as well as from the defensive side, how to stop such attack.

Cyber Kill Chain:

The term kill chain was first used in the military which is related to the structuring of an attack, which includes identification of the target, getting a foothold in the organization, attack timing, and decision, destruction of the target. Though this process is not universal but is accepted by the information security community and converted into the part of the cyber kill chain to better understand it which can be useful to break the kill chain in different stages.

F2T2EA:

• Find: Locate the target.

• Fix: Fix their location, make it difficult for them to move.

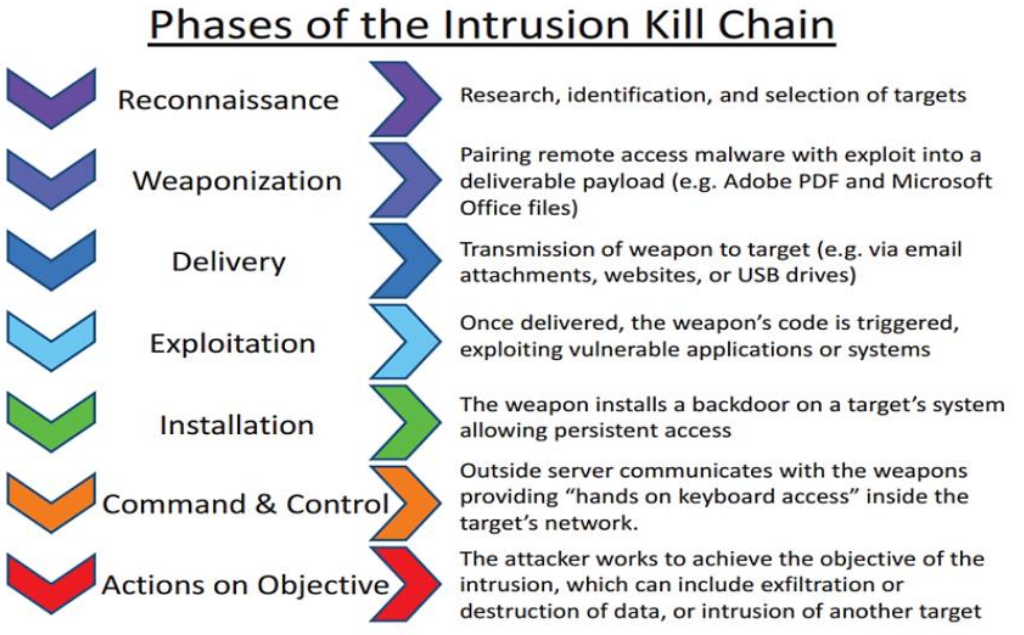
• Track: Monitor their movement.

• Target: Select an appropriate weapon or asset to use on the target to create desired effects.

• Engage: Apply the weapon to the target.

• Assess: Evaluate the effects of the attack, including any intelligence gathered at the location.

Now we will look at the different phases of cyber kill chain part of which mention below, is majorly derived from the Lockheed Martin which was first published by them in 2011. Since then it has been adopted by many organizations. Cyber kill chain reveals different phases of a cyber attack, from the initial stage of reconnaissance to the last stage of data exfiltration. This has been also used as a tool for the management to understand the phases of cyber attack to continuously improve their defensive measures. According to Lockheed Martin, these phases threats must pass through the model which is shown below


Phases of the Intrusion Kill Chain
Reconnaissance
Research, identification, and selection of targets
Weaponization
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation
The weapon installs a backdoor on a target's system allowing persistent access
Command & Control
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective
The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

CHAPTER 3

OPINIONS IN CYBERSECURITY

3.1 CITIZENS ON CYBERSECURITY IN GENERAL:

The Cyber Security Strategy proposed by the EU in 2013 notes that one of the main challenges in cybersecurity is the fact that cybercrime is high-profit and low-risk, and there is a lack of accountability which criminals often exploit. Cybercrime is now one of the fastest growing forms of crime with more than one million people worldwide falling victim each day. In order to combat cybercrime and increase the efficiency of cybersecurity, the Strategy recommends a coordinated collaborative approach stating that "security can only be ensured if all in the value chain (e.g. equipment manufacturers, software developers, information society services providers) make security a priority".

Making a coordinated effort across many sectors to boost cybersecurity with the aim of preventing cybercriminals from intruding into information systems, stealing critical data or holding companies to ransom may significantly reduce the potential of a cyberattack disrupting the supply of essential services we take for granted such as water, healthcare, electricity, or mobile services. However, a coordinated approach will not be successful without public engagement.

The Strategy accepts that citizens need to have trust and confidence in the people and businesses which design, control and operate security technologies in order for citizens to adopt and engage with new technology. The following section provides an overview on empirical research related to attitudes and opinions of EU citizens regarding cybersecurity in general. Therefore, we carried out a research on projects and surveys provided by the EU.

It became apparent that the attitudes of citizens regarding cybersecurity are addressed, either to a greater or lesser extent, in many projects. The most relevant points are summarized below. On account of the sufficient number of findings in this research step,

an additional literature search was not required (in contrast to the health, business and national security spheres).

'Special Barometer 359', conducted in 2011, reveals that four in ten internet users in the EU use strategies and tools such as anti-spy software to reduce unwanted emails and spam, and/or try to ensure that a transaction is protected by looking out for a security logo or label. One fifth of the internet users change the security settings of their browser to increase privacy and avoid providing the same information to different sites. Other "protection techniques" are cited by less than 15% of Europeans. 22% of internet users change the security settings of their browser to increase privacy and only 12% use a dummy email account.

These numbers are very low and appear to be influenced by the security company in charge of the analysis of the data collected, i.e. citizens' opinions vary depending on whether cybersecurity is operated by a public institution or a private institution. For example, 78% of Europeans trust health and medical institutions, 70% trust national public authorities such as tax authorities and social security authorities. 22% trust internet companies such as search engines, social networking sites, and email services. Seven in ten Europeans are concerned that companies may use their personal information for a purpose other than that for which it was originally collected without informing the citizens themselves (e.g. for direct marketing or targeted online advertising).

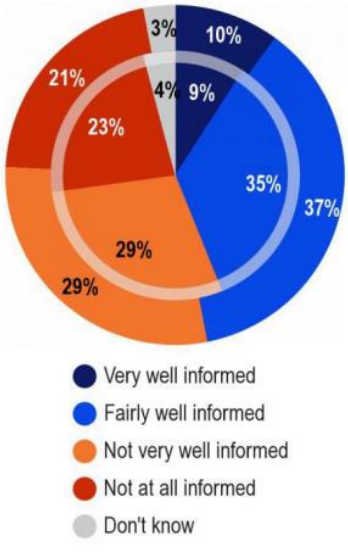
In the event of a cyberattack or information leak, nine in ten Europeans want to be informed by a public authority or by a private company if information held about them has been lost or stolen. 'Special Eurobarometer 423', conducted in 2014 and published in 2015, updates the previous study 'Special Eurobarometer 404' from 2013 about cybersecurity. Simultaneously with an increasing number of internet access (from 72 to 76%), devices (especially smartphones from 35 to 61% and tablets from 14 to 30%) and online activities (e.g. social networks from 53 to 60%, buying goods or services from 50 to 57%), the concerns of EU citizens regarding internet transactions and cybercrime are rising.The most common concerns are about the misuse of personal data (from 37 to 43%) and the security of online payments (from 35 to 42%); only 18% (2013: 23%) of the respondents have no concerns.

Asked about their agreement to concrete statements about attitudes to cybersecurity, 89% (2013: 87%) states that they avoid disclosing personal information and 85% (2013: 76%) perceive an increasing risk of becoming a victim of cybercrime. Concerns that personal information is not kept secure by websites are shared by 73% (2013: 70%) and are

somewhat lower with regard to public authorities (67%; 2013: 64%).The results of querying a list of concrete cybercrimes show that the majority of internet users have growing concerns about different sorts of crimes; they fear identity theft (68%; 2013: 52%), discovering malicious software on their device (66%), being a victim of bank card or online banking fraud (63%, 2013: 49%) and a hacked social media or email account (60%, 2013: 45%).

The number of respondents who changed their online behaviors because of security concerns increased since 2013 from 81 to 88% (largest growths: using anti-virus software from 46 to 61%, not opening emails from unknown people from 40 to 49%). Even though only 47% (2013: 44%) feel well informed about the risks of cybercrime, around three in four internet users state to be able to protect themselves sufficiently. In case of becoming a victim of cybercrime, the respondents would, in most cases, contact the police (depending on the sort of crime, between 37% by a hacked social media or email account and 84% in case if identity theft), followed by website or vendor and the internet service provider.

QB1. How well informed do you feel about the risks of cybercrime?



In 'Special Eurobarometer 432' from 2015, it becomes apparent that EU citizens perceive cybercrime as a significant threat in general, but they consider themselves also better

informed: the open question for the (three) most important challenges to the security of the EU was answered by 12% with "cybercrime". By the rating of the five main challenges, cybersecurity was with 80% the third most important internal security challenge; 63% of the respondents believe that cybercrime will increase. For EU citizens, the entities that play an important role in ensuring security against cybercrime are the police (70%), the judicial system (64%), the army (47%) and the citizens themselves (46%) – although only 46% agree that the police are doing enough to fight cybercrime, while 40% do not think so.

Privacy concerns are an issue for EU citizens. For example, according to interview meetings conducted in 2007 within the EU project PRISE (which considered mass surveillance methods in the interests of national security), 85% of EU participants agree that privacy should not be violated without reasonable suspicion of criminal intent and 80% feel that it is unpleasant to be under surveillance stating that "participants in general weigh privacy higher than security". Participants differentiate serious crime from petty crime (e.g. speeding or shoplifting): petty crime is not considered a legitimate reason for privacy infringement whereas serious crime (unspecified) is.

The issue of access is again raised in the context of what information is being collected by security companies and what harm could come from the potential misuse of same. The report also notes that EU citizens believe "physically intimate technologies are unacceptable, [the] misuse of technology must be prevented and function creep is not acceptable". In 2012, PRESCIENT found that the majority of EU citizens lack an adequate understanding of how data processing and security utilities operate, stating that this limits the ability of the individual to "rationally balance each transaction for benefits and consequences". Participants reaffirm the opinion that they are uncomfortable with the idea of being under surveillance.

The relevant EU projects presented below are all part of the 7th Programme for Research and Technological Development, in which research projects regarding specific thematic areas were generated. The CONSENT, SMART, and RESPECT projects all deal with different perspectives on privacy and new technologies such as security and surveillance, therefore their implications are brought together. The CONSENT project ran from 2010 until 2013 and attempted to analyse online consumer behaviour by, amongst others, querying consumers' attitudes towards personal privacy. A part of the project was a study ran in 2011 about awareness, values and attitudes of user generated content (UGC) website users towards privacy. With a combination of quantitative and qualitative research, 8,641 individuals from 26 EU countries were questioned.The respondents are "above-average frequency internet users": 87% created an account with a social networking site.Among

the reasons why they would not use these accounts, trust issues only plays a minor role (8%), a bigger role among the reasons for deleting the accounts (30%).The types of information that they disclose the most are name (83%), email address (79%), and photos of themselves (68%).

Nevertheless, the disclosure of personal information is perceived as high risk (5.2 - 6.1 on a scale 1 - 7); for the respondents it is likely to happen that information being shared is used to send you unwanted commercial offers (81%), that it is used without the user's knowledge (74%), and that it is shared with third parties without the user's agreement.74% are aware that the information they include on a website may be used for other purposes, 53% are changing the privacy settings on UGC websites often or always, 18% rarely or never. Only 11% of the respondents state to always read terms of conditions of a website; the majority rarely or never read them. 89% of those who read them indicate that they do not (fully) understand the privacy policies. The aim of the SMART project, which ran from 2011 until 2014, was to examine social and legal consequences of adopting automated, "smart surveillance" systems by public bodies.Part of the project was an evaluation of citizens' attitudes towards smart surveillance and privacy via 42 focus group discussions with 353 participants in 14 European countries. The participants showed a high awareness of the current state of surveillance, especially as users of mobile devices and internet services.

Individuals, at least in part, are considered as responsible for their own personal (online) data. Surveillance in public places, unlike private places, is mostly accepted, especially if the monitoring is transparent; surveillance for safety reasons is more accepted than for commercial objectives. Dataveillance is perceived as a threat to privacy, even though most participants believe that the recent legal restrictions are sufficient. The acceptance of data sharing and collecting is dependent of the type of data (mostly unacceptable by sensitive data, anonymized data more accepted), the purpose of use (e.g. acceptable by lifesaving circumstances), the conducting entity (state actors in general more trustworthy than private actors) and a given consent. The approval of surveillance technologies differs between different types: the more intrusive the technology, the bigger the aversion to it. The concept that more surveillance leads necessarily to more security was opposed by the majority.

Building on the results of CONSENT and SMART, RESPECT explored the European citizens' awareness and acceptance of surveillance systems and procedures, with additional questionnaires and interviews in 28 European countries (5,361 participants) in 2013-2014.It becomes apparent that the majority have knowledge about the different types of

surveillance and the reasons for it (especially detection, prosecution and reduction of crime).23% of the respondents feel secure due to surveillance whereas 37% feel insecure; they perceive a lack of control over their personal information and mistrust government agencies and, to a greater extent, private companies. Surveillance by government agencies is more accepted (just 6%: "not acceptable under any circumstances") than by private companies (16%: "not acceptable under any circumstances"); the approval decreases even more if the surveillance happens without knowledge of the affected people. Moreover, the acceptance is dependent on the location: both CCTV and geolocation surveillance are least accepted in the workplace, most accepted in clinics and hospitals.

While the majority believe that surveillance takes place often or all the time (depending on the type of technology), only the minority feel well informed and confident about the effectiveness of laws and regulations and just a few respondents changed their behaviors due to surveillance. Social benefits (protection both for the individual citizen and the community) and social costs (limitation of rights, violation of privacy and control over personal data, misuse and misinterpretation, discrimination and stigma) of surveillance are both perceived without balancing them against each other.

The EU projects SurPRISE, PRISMS and PACT also belong to the FP7 programme and ran between 2012 and 2015. They aimed to examine the relationship between security and privacy, especially the idea of a "trade-off" between these values.Not only were they all acknowledged in the above-mentioned research of RESPECT, but they also organised a joint final conference about "Citizens' perspectives on surveillance, security and privacy".Looking at the adoption of security technologies in surveillance and how they are viewed by citizens, the SurPRISE project investigated European attitudes towards the employment of surveillance-oriented security technologies (SOSTs): smart CCTV, deep packet inspection (DPI) and smart phone location tracking (SLT). In 2014, it found that citizens would prefer if SOSTs were evaluated before implementation, paying particular attention to the purpose, appropriateness, cost, and impact of SOSTs. Participants would also prefer verification of what data and information is being collected by SOSTs, be aware of who is responsible of such data and for what purpose the data is being collected. Participants comment on the intrusiveness and usefulness of each SOST: all three SOSTs are considered useful but highly intrusive, with DPI receiving the highest perceived level of intrusiveness (66% of participants).

In relation to effectiveness and future use and potential abuse of DPI, 43% of citizens state that DPI is an effective security tool despite 66% feeling uncomfortable with the use of DPI. 84% are worried about the extension and future use of DPI and 70% of participants

share the opinion that SOSTs are likely to be abused. 70% are concerned about extensive information collections, 63% fear that information held about them might be inaccurate, near to 80% fear that their personal information might be used against them and 91% are concerned that their information is shared without their permission. 50% of participants disagree with the statement "if you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" with only 34% agreeing with this statement. What is interesting is that 52% of the "nothing to hide" supporters are at the same time concerned that too much information is collected about them, which is contradictory. Some participants also feel that SOSTs are forced upon them.

In 2014, the PRISMS project explored EU citizens' perceptions of privacy and security issues, gathering data from focus groups and 27,000 respondents (1,000 per EU27 member state).32% of participants are worried about someone hacking into their computer, 62% of participants feel that it is important that they have the freedom to use the internet anonymously, and 81% state that it is important that they know who has information about them.80% of participants state that internet service providers (ISPs) selling customer information should not occur and 75% of respondents believe that this practice threatens people's rights and freedoms.Again, citizens distinguish between security technologies and practices operated by public and private sector institutions: citizens have more trust that public authorities will respect citizens' right to privacy and data protection and, similarly to previous studies, citizens oppose covert surveillance practices and secondary use of data, especially for commercial purposes.This study also affirms that citizens seem to present a high level of resistance to private sector actors who collect and process personal data and, while a concern for security decreases resistance, a high level of trust in institutions also decreases resistance.

In 2013, the PACT project examined the European citizens' perception of the relation between privacy, fundamental rights, and security by surveying 27,000 EU citizens (1,000 per EU27 member state) on their attitudes towards scenarios regarding travel, internet service provider, and health. It becomes apparent that the attitudes towards the collection and storage of personal data as well as the access to data are dependent on the specific context. The collection and storage of personal data is rather accepted in the context of traveling (presence of CCTV) and health (storage on devices or systems), but not on internet usage (especially in the long run).The respondents are averse to access to CCTV and internet usage data by the police (especially outside the home country); an EU-wide access to health data is accepted, but for medical personnel only.Moreover, the study shows a correlation between general attitudes towards privacy, surveillance and trust and their

chosen preferences, which rejects the trade-off model of security and privacy. For example, a traveling person who is concerned about misuse of data shows weaker preferences towards CCTV cameras than somebody with concerns about misuse of security measures for sexual or racial harassment.

The research in empirical studies regarding attitudes and opinions towards cybersecurity seems to show that EU citizens perceive an increasing threat of cybercrime. There is a number of stated risks (e.g. identity theft, online fraud), but the biggest one by far is privacy violation and loss of data control, especially the misuse of private data. The perception of surveillance depends on different factors: the entity and context of surveillance, the sort of data and the level of transparency about the surveillance methods. Transparent collection of non-intrusive data for security reasons by public authorities meets with the highest acceptance, while non-transparent collection of sensitive data by commercial institutions receives the lowest acceptance. The given consent of the affected citizens is perceived as crucial. There is an awareness about both the social benefits and the social costs of data collection and surveillance. The trade-off model between security and privacy is rejected to a large extent.

For most of the respondents, the importance of cybersecurity measures is constantly increasing. The vast majority wants to be informed about cybersecurity risks, but only a smaller part feels sufficiently informed. The trust in authorities which ensure cybersecurity shows a broad range: while trust in public authorities and medical institutions is moderately high, trust in private authorities and commercial institutions is low. In general, trust in sufficient legal restrictions regarding cybersecurity and data protection is very high. The responsibility for cybersecurity is not just attributed to institutions, but also to the individuals themselves. However, the changes in online behaviour and processing of personal data are not carried through: some security measures, e.g. changing of private settings, are more popular than others, like reading terms of conditions before accepting them. It appears that the average knowledge about the concrete possibilities and functionalities of cybersecurity measures is deficient. Therefore, more information about cybersecurity risks and concrete measures should be provided for the broad population.

3.2 CITIZENS ON CYBERSECURITY IN HEALTH:

An important survey regarding attitudes towards data is to be found in ‘Flash Eurobarometer 225’. In 2008, EU citizens were asked, among others things, about their trust in organisations concerning data protection. They perceive that their personal data is best protected by medical authorities, e.g. medical services and doctors (82%), whereas

insurance companies are less so (51%), and private companies, e.g. mail order companies, are the least trustworthy (24%). In 2010, a part of the survey for 'Special Eurobarometer 341' polled the attitudes towards biobanks. The most preferred group to protect public interest in the use of biobanks are medical professionals (39%), the second one researchers (32%), the third one public institutions (26%).67% state that researchers should ask for informed consent for every new piece of research (18% "ask for permission only once", 6% "no need to ask for permission").The question "Would you be willing to provide information about yourself to a biobank?" is answered by 46% with yes and by 44% with no.Respondents are mostly concerned about the collection of their personal genetic profile (34%) and personal medical records (33%), while 28 % are not concerned at all about personal information being stored in biobanks. However, 53% agree that the exchange of personal data and biological materials tissue across member states should be encouraged (while 32% opposed).

Another relevant survey is 'Special Eurobarometer 359', conducted in 2011. Being asked which information they consider personal, the respondents name medical information (patient records and health information) as the second most personal (74%) after financial information (75%). Appropriately, the percentage of people disclosing their medical information on the internet is very low at 5% (in comparison: name is 79%, personal photos is 51%). Similarly to 'Flash Eurobarometer 225', the trust in different authorities is addressed: health and medical institutions are deemed the most trustworthy authorities regarding protection of personal data with 78%. In comparison: the second most trustworthy authorities are national public authorities with 70%, the least trustworthy authorities are internet companies (e.g. search engines, social networking sites) with 22%. After being asked whether their specific approval should be required before any kind of personal information is collected and processed, 74% say in every case, and 8% in cases regarding sensitive information such as health information. The vast majority (88%) affirm the request for whether genetic information (e.g. DNA data) should have the same protection as sensitive data.

According to the CONSENT study from 2011, any disclosure of personal information is considered as risky: sharing of data without knowledge or consent is perceived as riskier (73 - 81%) than personal risks, e.g. fraud or discrimination (23 - 32%). Regarding which types of information they already disclose online, just 1% name medical information. From the SMART project (2011-2014), it appears that the collection and sharing of sensitive personal data, such as health data, is unacceptable to the majority. However, under certain (especially life-saving) circumstances, the usage of confidential information is deemed

acceptable. Moreover, it becomes obvious that the level of acceptance is dependent on the type of technology. Technologies involving the physical sphere, e.g. biometrics, are perceived as especially unacceptable. The empirical data from RESPECT in 2013-2014 show that the majority feel that they have little or no control over their personal information gathered with surveillance measures, and that there is a big risk of data misuse and misinterpretation.However, we must note that it was not clear in the questionnaire whether personal information included health information.

Part of the Surprise project was the consultation of EU citizens via workshops and questionnaires, in order to find out their understanding and attitudes towards security and privacy. In 2014, when asked what the core of privacy is, participants of the workshops name sensitive data (e.g. health information, sexual orientation), which should not be intruded upon. As for the data gathered by PRISMS in 2014, they show that regarding healthcare, there is a high concern about general socio-economic phenomena such as healthcare. Control over personal data (e.g. health) is in general of great importance. Part of the survey was the participants' opinions about scenarios regarding specific security technologies. The first scenario about airport body scanners describes a person whose colostomy bag is detected and who has to explain it to the security staff. The situation is perceived as difficult but acceptable given the security risks; while options for more privacy are discussed, a complete stop of detection is not considered due to security risks.In another scenario, a person receives a letter with doctors' recommendations for flu vaccination based on the government monitoring of internet searches and communication. Hereby, many participants are concerned about government monitoring general internet usage.

In a third scenario, a person voluntarily provides a sample of his DNA to a company for medical research, but then learns that the company has been asked to share the samples with the police for use in criminal investigations. While DNA technologies are considered useful in solving crimes, the idea of sharing such sensitive data make the participants uncomfortable. Therefore, consent for sharing data with the police appears to be crucial; the option to sell this information for profit is widely seen as unacceptable. The uncertainty of what will happen with the information in the future and how the legislation might change plays an important role.

One of the PACT scenarios was the choice to purchase a device or service for storing health information. In 2013, it becomes apparent that, in relation to other technologies such as CCTV, the storage of health data is mostly accepted. The majority of the respondents would prefer a device or service that allows, in addition to basic health data (e.g. blood

group, allergies, diabetic status), storage of personal identification data and data on lifelong health conditions (e.g. asthma, disabilities, cancer), but they oppose to a storage of data relating to all other health conditions and medical history.The perceived trustworthiness of different authorities regarding access to health information is widely ranged, though: an additional access by paramedics is preferred, but not by fire and rescue personnel; the participants are adverse towards non-state actors (e.g. insurance providers, pharmaceutical companies).

Number	Hypotheses	Findings
H3.1	Respondents prefer a device/system with enhanced health or personal identification information compared to those with only basic health status information.	Reject: Czech Republic, Lithuania Accept : all other countries
H3.2a	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics	Accept: Slovenia Reject: others
H3.2b	Respondents prefer that only doctors and nurses have access to information compared to access also by paramedics, non-medical emergency personnel or any other state or private institutions.	Accept: all countries
H3.3	Respondents do not prefer device/service that can provide wider access outside their own country (EU/worldwide).	Accept: Austria, Czech Republic, Slovakia, age >65 Reject: all other countries
H3.4	Respondents do not prefer a health-records device/service to which health insurance providers, pharmaceutical companies and researcher could have access.	Accept: all countries
H3.5	Respondents prefer device/service that is free over a device/service that charges a fee per month.	Accept: at the device level Reject: WTP for some data and access options

Biometric technologies for personal authentication can be in some aspects relevant for the health sphere. Two studies were found which surveyed the attitudes of EU citizens towards biometrics: the multilevel-multimethod approach of BioSec in which an attitude survey across Europe took place (204 questionnaires in Finland, Germany, and Spain), and a study about regional differences in the perception of biometric authentication technologies. Although the use of biometric technologies is mostly accepted due to their benefits, e.g. as an authentication method, there are also concerns due to the uncertainty for what exactly (else) the technology will be used for.

Especially, the storage of biometrical data, which may include information about physiological condition and health, raises concerns: half of the respondents from the UK are not convinced that their biometric information is stored in a secure way. The cross-European survey shows similar results: while there is no agreement regarding which storage medium is preferred for the data (a central database or a personal smart card), around 33% of the respondents cannot decide or do not want their biometrical data to be stored at all.

As it already became apparent in 'Special Eurobarometer 341', the field of biobanks can be interesting for cybersecurity in health. Two pertinent studies could be found in academic research: a focus group study on biobanks in the information society (18 focus group discussions in Austria, Finland, and Germany) and a multi-method approach about publics and biobanks115 (with focus groups in the Netherlands and Austria as well as 15,650 questionnaires in EU27 member states, Croatia, Iceland, Norway, Switzerland, and Turkey).

The willingness to participate in biobanking by giving personal data through donation of e.g. blood, tissues and body fluids (i.e. including DNA data) is relatively high. The respondents state a broad acceptance of usage especially for research due to the perceived societal benefits. However, the majority would prefer to be informed and asked for consent for every specific use of their data, even though they are aware of the limited possibility to do so. They trust mostly in data security through public and state organisations, but not with private organisations.

Not only commercialization, but also internationalization of biobanks (especially storage of data) is perceived as risky. The biggest concerns regarding biobanks are the future handling of sensitive data: the uncontrollability of future developments and therefore the possible usage of the stored data (e.g. for discrimination) is viewed very critically.

In the empirical studies found, it becomes apparent that the handling of health data plays an important role. Health data is considered as being an especially sensitive form of personal data. Health data includes every data that provides information about the health condition of a person. In a broader context, it can also include biometrical and genetic data. The willingness to accept the recording, processing, and storing of health data is dependent on different factors. The transparency about the purposes of personal data and the way it is handled is perceived as crucial.

The respondents in the aforementioned studies seem to agree to a certain extent on which authorities can be trusted in dealing with health data: health authorities, especially public

institutions, are trustworthy – in contrast to commercial institutions (e.g. health insurance agencies, pharmaceutical companies) which generally are more expected to misuse data. The more databases and networks are connected internationally, the less they are accepted.

Control over own privacy and data is stated important; nevertheless, the majority of respondents are aware of the benefits of electronic records of health information: not just security aspects, but also gained knowledge (e.g. for medical research) is highly appreciated. Most worries about potential risks regarding health data concern future developments about who is handling the currently stored data and for what purposes. This lack of confidence is widespread especially with regard to data that contains information about the identity of the data subject. In the empirical research about cybersecurity in health, it becomes apparent that there are only a few studies dealing with opinions and attitudes of EU citizens. Moreover, the few results that could be found appeared to be focused mostly on attitudes towards (health) data protection and privacy. Other aspects of cybersecurity in health seem merely to play a minor or even no role at all.

3.3 CITIZENS ON CYBERSECURITY IN BUSINESS:

Cybersecurity utilities are wide ranging so much so that they have been afforded elaborate definitions such as the following: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets." 126 We used this definition as a benchmark with the aim of capturing all relevant empirical data pertaining to EU citizens' attitudes towards cybersecurity utilities from the period 1996 to 2016.

Lack of trust in privately run businesses is affirmed in 'Special Barometer 359'. In 2013, for example 39% of participants included in this study trust shops and department stores; 32% trust phone companies, mobile phone companies and internet service providers; and 22% trust internet companies such as search engines, social networking sites and e-mail services. Surveillance and monitoring concerns via payment cards, mobile phones or on the internet were also raised, with seven in ten Europeans worried that private companies are using

their personal information for a purpose other than originally intended (a process known as function creep), and without informing the citizen (e.g. for direct marketing or targeted online advertising).

While 'Flash Eurobarometer 225' reiterates similar concerns, it also highlights that citizens have the greatest levels of distrust in mail order companies. 133 In 2008, 82% of internet users reason that data transmission over the web is not sufficiently secure, with a third of respondents stressing that suspicious persons should be monitored (27%-35%) and one in five (14%-21%) would like stricter safeguards. 92% of Greek and Cypriot respondents who use the internet feel that their personal data is not sufficiently secure, while very few believe that it is (6%). In contrast, 40% of Danish internet users feel transmitting data online is secure and respondents who express uncertainty about the efficiency of the security oriented technologies are male and from the younger age groups.

In relation to the potential privacy vs. autonomy conflict, the PRISE project found in 2007 that EU citizens weigh privacy higher than security, while 80% of them feel that it is unpleasant being under surveillance. In relation to the threat of crime and terror, citizens are more accepting of security technology when the risk of crime is increased. In respect of security technology, participants are concerned with its effectiveness and that there is potential for misuse by criminals, commercial interest and governmental institutions. Identifiable information and access are again raised as concerns by EU citizens. They feel that new security tools should be subjected to public scrutiny before implementation.

PRISE concludes that

1) "physically intimate technologies are unacceptable, misuse of technology must be prevented and function creep is not acceptable"

2) security technologies are more acceptable when there is proportionality between security gain and privacy loss, when security is under strict control (to prevent misuse by the people with access to data) and when privacy infringing security technologies are the last option (previous methods must be measured and found less effective prior to implementing privacy infringing technologies).

In relation to security technologies, the PRESCIENT project found in 2012 that new technologies are not understood by the general public and access to new security technology and its uses is invisible to the average citizen – therein is where cybersecurity risks manifest. It revealed that EU citizens have a variety of concerns relating to

cybersecurity in business but interestingly, some EU citizens are more concerned than others. For example, data collection, data security, unauthorized or inappropriate use of data, and illegitimate disclosure of intelligence data are issues raised by citizens from Cyprus, Germany, Ireland, Italy, Slovakia. Concerns relating to the disclosure of information on the internet or to third parties regarding the public facility services are raised by Swedish and Latvian citizens. Employeremployee relationships, human resources, monitoring or surveillance of employees in the workplace and employees right to privacy and data protection in the workplace are issues raised by citizens from Belgium, Denmark, Portugal, Slovenia, Sweden, whereas the financial sector in general and the leakage of financial data are raised by Danes and Slovaks. Belgians and Slovenians are concerned with spam and viral marketing and direct marketing and Germans are also concerned with non-public sector and telecommunications. Slovaks too are concerned with the use of loyalty cards and the legitimate use of biometric data, while Danes and Slovenians also have concerns regarding the use of social networking sites. We note that in the United Kingdom between 2007 and 2011 citizens' trust in online companies decreased by 8% and trust that organizational practices provide sufficient protection of personal information decreased by 5%.

This project looked at surveillance-oriented security technologies (SOST) including smart CCTV, smartphone location tracking and deep packet inspection (DPI). DPI is the most relevant SOST as

1) it is used in cybersecurity as a packaging filter through which information is scanned for non-compliance, virus, etc.

2) it can be used by businesses for internet data mining (the process of collecting and using large sets of data for actions such as choosing the best customers for targeted mailings or analysing a shopping cart), eavesdropping and internet censorship. According to SurPRISE data from 2014, citizens suggest SOSTs should be evaluated before implementation, clarifying their purpose, appropriateness, cost and their potential impact. Participants would like verification on what data is being collected, who is responsible for such data, and for what purpose is the data being collected. SOSTs are considered as useful but highly intrusive and interestingly DPI is perceived as most intrusive. 43% of EU citizens who participated in this study state that DPI is an effective security tool and 66% feel uncomfortable with its use.

84% are worried about the extension and future use of DPI with 70% believing that SOSTs are likely to be abused. 70% are concerned about extensive information collections, 63%

fear that information held about them might be inaccurate, near to 80% fear that their personal information might be used against them and 91% are concerned that their information is shared without their permission. 50% of participants disagree with the statement "if you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" with only 34% agreeing with this statement.52% of the "nothing to hide" supporters are at the same time concerned that too much information is collected about them, which is contradictory.

The PRISMS project found in 2014 that 62% of respondents to the survey think that it is important to be able to use the internet freely and anonymously, and 81% state that it is important that they know who has information about them. It also reaffirms that – as seen in 'Special Barometer 359' – citizens distinguish between security technologies and practices operated by public and private sector institutions. Citizens have more trust that public authorities will respect their right to privacy and data protection when compared to profit-oriented companies; they oppose covert surveillance practices and the secondary use of data, especially for commercial purposes; there is a high level of resistance to private sector actors who collect and process personal data.

3.3 CITIZENS ON CYBERSECURITY IN POLICE AND NATIONAL SECURITY:

While people do not seem to like the privacy vs. security trade-off situation, it is hard to deny that this trade-off is often present when it comes to concrete measures. In 2015, SurPRISE further discussed the often-cited assumption that the gain of additional security leads to a loss of privacy. "The trade-off model is based on the assumption that the employment of security measures requires privacy intrusion in order to come to a certain level of security. This logic inherently operates as if privacy intrusions would be the only and inevitable option to effectively improve security." In order to minimize the trade-off in the case of conflicting security and privacy goals, it is important that a good knowledge of the involved technologies and their effectiveness exists. One of the key findings of PRESCIENT in 2012 has been the fact that citizens often lack understanding of the techniques involved in security measures, especially of security measures deployed on a large scale by state actors such as biometrics. "Thus the consequences of each technology are not necessarily easily comprehensible, or even directly relatable to that technology."

We must therefore conclude that it is not sufficient to define values: adequate and unbiased information need to be supplied, not only to the decision makers but to the citizens as well. For all technically-savvy people it is important to take this into account when implementing value-sensitive technologies. This is not only relevant for state actors but for

the private sector as well. It is not sufficient for a security company to say "we adhere to the respective local laws" but it should instead relate to a common set of values for the development and operations of their technology. The fact that the private sector is a player in this domain as well is reflected by one finding of SurPRISE in 2014, namely the reluctance of many persons against the involvement of the private sector in the domain of surveillance.

"Acceptable SOSTs [Surveillance-Oriented Security Technologies] are technologies operated only by public authorities for the sake of the public interest. The participation of private actors in security operations should be limited and strictly regulated."One of the most often cited attitudes towards privacy is "those who have nothing to hide have nothing to fear", a statement that falsely reduces privacy to a form of secrecy aiming at hiding things.The authors of PRISE state another interesting fact that the public expects the policy makers to foster a discussion about new technologies before they are introduced, and to state clear limits on the technologies in order to prevent a function creep.

This discussion should be as broad as possible.In 2007, the study found a certain ambiguity towards the role of the state and the use of PETs (Privacy Enhancing Technologies). "When it was pointed out that some technologies could prevent investigation of specific crimes such as distribution of child pornography, they gained even less acceptance." Another important factor described by PRISE was the fact that the public only accepts security measures if they are perceived as effective. This is also valid for all privacy measures. PRISE concludes and recommends a dynamic and regularly reassessed approach when it comes to security and privacy measures: "The implementation of security technologies and legal regulations must therefore be reassessed regularly and precautions for the required flexibility to permit the withdrawal of inefficient and infringing measures and technologies should be taken.

The SurPRISE project tried, amongst others, to measure the perception of the intrusiveness vs. the effectiveness of so-called surveillance-oriented security technology (SOST). In 2014, SurPRISE analysed the following SOSTs: smart CCTV, deep packet inspection (DPI) and smartphone location tracking (SLT). One interesting finding is that there is a relation in the perception of a technology between its effectiveness and its intrusiveness: "Despite of the differences in particular, the effectiveness and intrusiveness of the SOSTs are interrelated: those technologies perceived as highly intrusive are also perceived as less effective."

Technology	Considered an effective national security tool (*)	Considered an appropriate way to address national security threats (*)	Feeling uncomfortable with the use of the technology
smart CCTV	64%	51%	39%
DPI	43%	about 40%	45%
SLT	55%	about 40%	66%
(*) % of participants strongly agreeing or agreeing that it is an effective technology.[182]			

This is a very interesting finding as, from a technical point of view, DPI was considered as being ineffective for national security compared to SLT and smart CCTV. When we consider the findings of PRESCIENT and PRISE, a certain part of these findings might be related to the fact that DPI is one of the most complex technologies with a high risk of function creep. However, DPI might be one of the most interesting technologies against certain threats to national security but it is most likely one of the most privacy intruding. If a state actor decides to do DPI, widely used cryptography is something that hinders this approach. It is interesting to note that none of the examined papers seems to focus on the role of the state when it comes to cryptography ("cryptowars", where states try to enable a decryption of communication or data by legal measures).

Technology	Security authorities are trustworthy when using the technology (*)	Security authorities do not abuse their power (*)
smart CCTV	36%	22%
DPI	36%	14%
SLT	46%	29%
(*) % of participants strongly agreeing or agreeing that it is an effective technology.[185]		

The weakening of cryptography would likely have much stronger security and privacy consequences than most of the other invasive technologies. We believe that not only technologies actively used by actors might endanger some core values but as well the fact that states try to weaken techniques for their own purposes. As von Liechtenstein already pointed out in 2002, this may have a major change in the balance between states and citizens: "The potential of cryptography to reorder citizen/government power relationships is already attracting the close attention of National Governments."

It is important that the public discussion does not only focus on the use of SOST but also on which PETs are available to what extent and if the state does not try to circumvent, ban

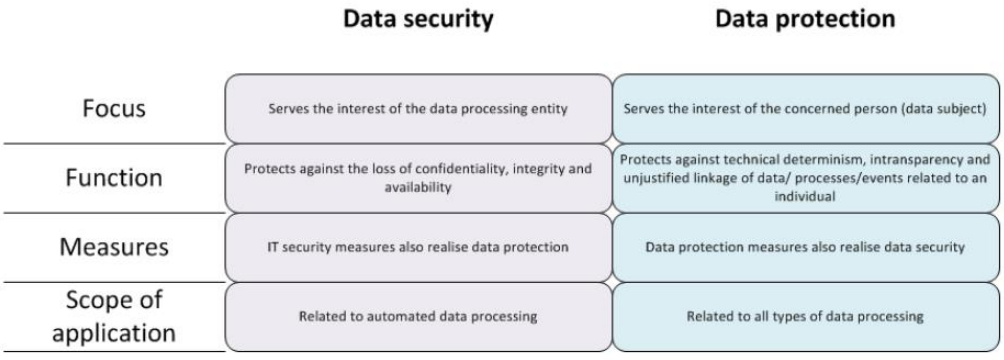
or weaken such technologies for the broad public for the sake of SOSTs. One of the most interesting research questions of SurPRISE was about the criteria that should be adopted when introducing new SOSTs. We are going to focus on the most important factors that seem to have a direct relation to potential values that should be considered by state actors. According to SurPRISE participants in 2014, "SOSTs are more acceptable if implemented in a context where information is provided to citizens on: a) where SOSTs are used, b) how SOSTs function, c) for what purpose they have been installed and d) who is in charge of managing the system. For us, this leads to one of the most important concepts in any democratic state.

Trust is something that can only be gained if all participants adhere to a common set of values. There are also security measures where the trade-off is less accentuated, but nevertheless subtle. For instance, consider the collection and analysis of metadata for the discovery of malware flows. On the one hand, the metadata collection has adverse effects on privacy. On the other hand, the detection of infected devices helps restoring the privacy of affected users. We believe that if in this example metadata collection would be forbidden out of, loosely speaking, "privacy concerns", the net effect on privacy would be negative: the damage to privacy caused by undetected malware would be greater than the (forbidden) privacy invasion due to cybersecurity software.

In summary, we believe that it is crucial to gain and maintain a holistic, value-based view on all topics and to avoid isolated views on singular problem blocks. A pronounced "privacy first" or "security first" attitude is unlikely to produce beneficial solutions for society. Finding good solutions and trade-offs is a laborious and ongoing process, which requires to assess a multitude of technologies and application scenarios with respect to their effect on the core values of a society.

Data Protection:

Data Protection is based on protection goals which can be derived directly from the applicable data protection framework. This protection goal based approach provides a more tangible concept to identify and implement measures needed to protect information related to individuals, while those measures are also useful to enhance cybersecurity. According to article 35(7) GDPR, the DPIA is required to provide at least:



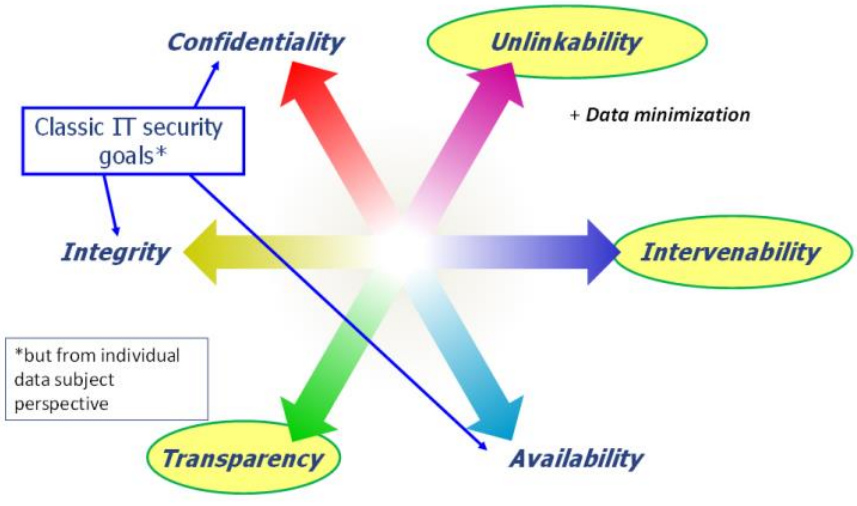
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph;

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Such an assessment requires the responsible entity to take into account the whole processing lifecycle, including all data, formats, IT systems, processes and functions.



In the IT security domain, the processing lifecycle is usually looked at from a risks assessment standpoint, while some classic protection goals are taken into account as well . This approach is called the classic CIA triad (for the protection goals confidentiality, integrity, and availability) and is commonly used by IT security experts to conduct assessments. However, these protection goals do not cover all data protection requirements, since the classic IT security perspective is driven by the desire of the controller to protect business data and assets. Data protection, however, goes further than that, due to its fundamental rights status, primarily considering the perspective of the individual (the data subject). Therefore, the classic IT security approach needs to be extended to a more holistic viewpoint, striving for tangible operational measures that protect not only business models, but also the fundamental rights of individuals in relation to privacy and data protection.

To close this gap and help with the translation of complex legal requirements into functional requirements, an extension of the original methodology has been made in the above-mentioned Standard Data Protection Model. Originally developed in Germany, it provides a methodology which is directly based on the GDPR and is thus useable all across the EU. Briefly summarized, three additional data protection goals supplement the IT security focused ones, namely: unlikability (data minimization), intervenability, and transparency.

These additional, privacy-focused goals can be used together with the classic IT security goals to assess and evaluate data protection and data security objectives and risks. Therein, they can be mapped exactly to the (often rather vague and broad) legal requirements of

the European data protection framework. This approach is strongly aimed at determining the needed operational measures to resolve data protection issues, but which have the potential to enhance cybersecurity as well. Therefore, it may be a candidate methodology to receive more widespread recognition internationally, besides the efforts of the above-mentioned IT security and cybersecurity focused institutions to raise the prevalence of already known security standards.

Perceived risks may not fully match real threats. Likewise, known security measures may not be the only ones in use, nor necessarily the most adequate. Moreover, these results might be influenced by the intrinsic bias towards privacy of some of the surveys, especially those focusing on ways to go beyond the traditional trade off between security and privacy. For citizens, the biggest risk associated to cybersecurity generally seems to be privacy violation and the loss of data control. People seems to trust more public authorities than private entities with their personal data. They also perceive the increasing threat of cybercrime. They feel insufficiently informed about cybersecurity risks, which highlights the need to improve awareness: more information about current risks and concrete (counter)measures should be provided to a broader public.

In the health sphere, citizens are especially sensitive to the handling of their health data. Consent and trust for the recording, processing, and storing of such data depend on the context. In the business sphere, citizens are also concerned with privacy infringements. There is a lack of trust in private businesses regarding the use of personal data, as well as a concern with internet and e-commerce security.

In the police and national security sphere, there is diversity in the perception of the role of the state and of value-sensitive technologies such as DPI. Citizens find national security measures more acceptable if they view the state as a guardian rather than an intruder, which depends on their experience and their country's history. Security technologies and their application scenarios should be carefully assessed before seeking public acceptance. However, we should not have to choose between (cyber) security and privacy, or any other value. We ought to keep a holistic view on all value-related topics.

Overall, most found data on citizens' perspectives relates to general issues of security and privacy. The cyber component of security is often not emphasized in the studies. Further research is therefore needed to cover other values, but also to investigate specific issues such as cybersecurity and health, or cybersecurity in business. Besides, longitudinal surveys could study the influence of news stories on public opinion. For instance, what are

acceptance levels of personal data collection before, during, and after privacy scandals (e.g. Snowden's revelations).

Does an attitude towards privacy leads to an attitude towards cybersecurity? The protection of personal information can also improve cybersecurity. For example, using a VPN when connected to a public hotspot (in an airport, in a hotel or in a shopping centre) prevents the communication to be eavesdropped by other users at this hotspot. In particular, personal identifying information is not visible anymore. Therefore, using a VPN can be seen as an attitude towards privacy. A VPN also prevents the interception and the stealing of the passwords at the hotspot. From this point of view, it is also an attitude towards cybersecurity.

Thus, privacy and some aspects of (cyber)security can be mutually reinforcing. However, a VPN can also be used to lure content providers about the actual geolocation of a user. This is a way to circumvent location dependent DRM and intellectual properties. Such a use of a VPN is an attitude against some particular cybersecurity measures. This example illustrates how an attitude can protect privacy and at the same time be an attitude both towards and against cybersecurity: the use of a VPN prevents some personal identifying information leakage and protects certain cybersecurity assets while endangering some others. Cybersecurity is too vague or too broad to be considered as a monolithic entity. It needs to be contextualized in order to assess the impact of a particular attitude, measure or action. Eventually, according to the Standard Data Protection Model, three new protection goals should be added to the CIA triad (confidentiality, integrity, availability): unlikability, intervenability, and transparency.

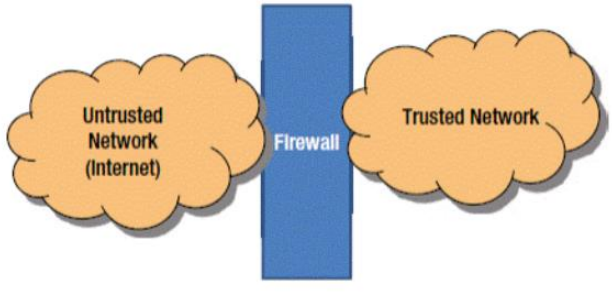
Ultimately, working towards value-driven cybersecurity goes beyond adding privacy requirements, although it is a first, significant and welcome step. Both citizens' perspectives and their direct involvement are crucial to enforce fundamental rights in the cyberspace and to contribute to a more secure, value driven information society.

CHAPTER 4

NETWORKS IN CYBERSECURITY

4.1 Firewall and Packet Filters:

Every small and big enterprise comprises the network of machines. They tend to communicate, sharing information, sharing resources, data in and out of the network. They are also connected to the internet. But once the machines are connected to the internet it opens all the ways for the outsiders or better to say hackers which has the malicious intent and start attacking the machines. This is the point where the concept of a firewall comes into the picture. In simple terms, a firewall can be explained as a wall built to protect from the fire and slow down its spread. In networks also it has a similar concept and understanding. A firewall intended to stop unauthorized users from accessing the network. The most common place to deploy the firewall is between the trusted and untrusted network of organization which typically is the internet



The term firewall has different meanings which are based on the implementation and purpose. That will be the place where the security policies are implemented. The firewall's external network interface card is the gateway to the internet. The purpose is simple; to protect what is there on your side of the gateway. A firewall is a device, operating system, or application program that enforces an access control policy between networks.

A firewall acts as a gatekeeper between your local area network and the internet. All traffic from in and out of the LAN must pass through the firewall. There needs to be some type of firewall installed in your network even if you are a home user having a broadband connection or high-speed connection.

Firewall setup can be done in different ways based on implementation and usage. You can purchase a hardware firewall which is basically a router with inbuilt firewall features. Also, most of the hardware appliances come with the web-based interface which will provide an easy interface to connect with firewall and setting can be easily configured. The purpose here to configure the firewall will enforce the policy which is defined during the configuration which will allow or deny the internet traffic based on those rules and policies configured. Security policies are all about the access control and authenticated use of private or protected use of the application, file services and programs.

Another way is to install a server computer and use it as the firewall. In large networks, it is sometimes hard to figure out where to place the firewall or perimeter. Perimeter is used to describe the location of the firewall inside the large networks (WAN). Let us discuss different types of firewall techniques.

Types of Firewall:

Packet Filtering: Packet filter firewall examines each packet that crosses the firewall and checks the packet according to the set of rules which are defined. If all rules are satisfied with the packet that it is allowed and if not then the packet is rejected. It is the very least expensive type of firewall. Packet filters work by inspecting the source IP address, destination IP address, a port number assigned to each service. The decision can be based on factors other than IP header fields such as ICMP message type, TCP SYN, and ACK bits, etc.

Packet filtering rule has two parts:

Selection criteria – It is used as a condition and pattern matching for decision making.

Action field – this part specifies an action to be taken if an IP packet meets the selection criteria. The action could be either block (deny) or permit (allow) the packet across the firewall.

Packet filtering is generally accomplished by configuring Access Control Lists (ACL) on routers or switches. ACL is a table of packet filter rules. As traffic enters or exits an interface, firewall applies ACLs from top to bottom to each incoming packet, finds matching criteria and either permit or denies the individual packets. As it is the most common firewall technique it has its own weakness. One of the biggest weaknesses of packet filtering is that it trusts that the packets themselves are telling the truth when they say who they are from and who they're going to.

Hackers exploit this weakness by using a hacking technique called IP spoofing, in which they insert fake IP addresses in packets and they send to your network. Another weakness of packet filtering is that it examines each without considering what packets have gone through the firewall before and what packets may follow. In other words, packet filtering is stateless. In spite of these weaknesses, packet filter firewalls have several advantages also.

Packet filters are very efficient. They hold up each inbound and outbound packet for only a few milliseconds while they look inside the packet to determine the destination and source ports and addresses. After these addresses and ports have been determined, the packet filter quickly applies its rules and either sends the packet along or rejects it.

Packet filters are inexpensive. Most routers include built-in packet filtering.

Stateful Packet Inspection: Stateful firewalls can watch traffic streams from end to end. They are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledges or established). It can tell if the MTU has changed and whether packets have fragmented. etc. Stateful firewalls are better at identifying unauthorized and forged communications.

Circuit Level Gateway: A circuit-level gateway manages connections between clients and servers based on TCP/IP addresses and port numbers. After the connection is established, the gateway doesn't interfere with packets flowing between the systems.

It is a networking proxy mechanism that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side without requiring direct IP reachability. The client connects to the SOCKS server at the firewall. Then the client enters a negotiation for the authentication method to be used and authenticates with the chosen method.

The client sends a connection relay request to the SOCKS server, containing the desired destination IP address and transport port. The server accepts the request after checking that the client meets the basic filtering criteria. Then, on behalf of the client, the gateway opens a connection to the requested untrusted host and then closely monitors the TCP handshaking that follows. The SOCKS server informs the client, and in case of success, starts relaying the data between the two connections. Circuit level gateways are used when the organization trusts the internal users and does not want to inspect the contents or application data sent on the Internet.

Application Level Gateway:

Application level gateway firewall systems are more advanced in terms of its features and working in compare to packet filtering or stateful packet inspection or circuit level gateway. It treats all the packets as equal level or equal priority. Application gateway firewall system knows the details that which application has generated these packets. In addition to that application level gateway is also worked as proxy servers.

A proxy server is a server that sits between the client machine and server machine. The proxy server will intercept the packet and will identify that the packets that are intended for the server machine or not and then it process them. For eg: web proxies are often stores the copies of the commonly used web pages in their local cache memory. When a user requests to access such pages which are present in the local cache memory that proxies itself reply to the user request, which in turns is very effective for the faster response. If it does not have the copy of the webpage it passes the request to the server machine.

Application level gateway is aware of the details, how a server machine handles TCP/IP requests and sequence of packets. So they can easily identify if the incoming packet is legitimate or fake or is part of an attack.

Application level gateway is more costly in terms of the price and cost of configuration and maintaining them. Application level gateway can slow down the network as it checks every packet in the deep which takes more time to process the packet before allowing them in or out of the network.

Firewall with Demilitarized Zone(DMZ):

The term DMZ originally arrives from the military where an area between two territories, military operations are prohibited. Similar way, many organizations are facing is how to

enable or allow to access to legitimate services of their organization to public services. While considering that not to compromise any other services of the organization. To achieve this the typical approach is to use a firewall to achieve the DMZ.

It will help to maintain and improve the security of the organization, by segregating the devices and machines on the opposite sides of the firewall. DMZ will act as a small and isolated network established between that internet and private network.

Some of the important functions of the DMZ are:

• All the traffic that goes in and out is inspected.

• Resources inside the DMZ are under continuous security monitoring to save them from being compromised from external cyber attack.

• It acts as a protective boundary for the private network

Packet Filtering:

Packet filtering is a process of allowing or blocking packets at one of the OSI layers which are usually a network layer, which also contains an IP header. IP header is used for routing packets through the internet as it contains all the important information of all protocols, IP address such as Source IP address and port, destination IP address and port as IP V4 is of 32 bit we have the similar IP V6 which is of 128 bit and contains similar information. There is another protocol apart from the IP which is TCP protocol.

<table>
<tr><th>bit offset</th><th>0-3</th><th>4-7</th><th>8-13</th><th>14-15</th><th>16-18</th><th>19-31</th></tr>
<tr><td>0</td><td>Version</td><td>Internet Header Length</td><td>Differentiated Services Code Point</td><td>Explicit Congestion Notification</td><td colspan="2">Total Length</td></tr>
<tr><td>32</td><td colspan="4">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td>64</td><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td>96</td><td colspan="6">Source IP Address</td></tr>
<tr><td>128</td><td colspan="6">Destination IP Address</td></tr>
<tr><td>160</td><td colspan="6">Options (if Header Length > 5)</td></tr>
<tr><td>160 or 192+</td><td colspan="6">Data</td></tr>
</table>

Important pieces of the TCP protocol header are the following fields:

• Source port: from which port the packet was sent.

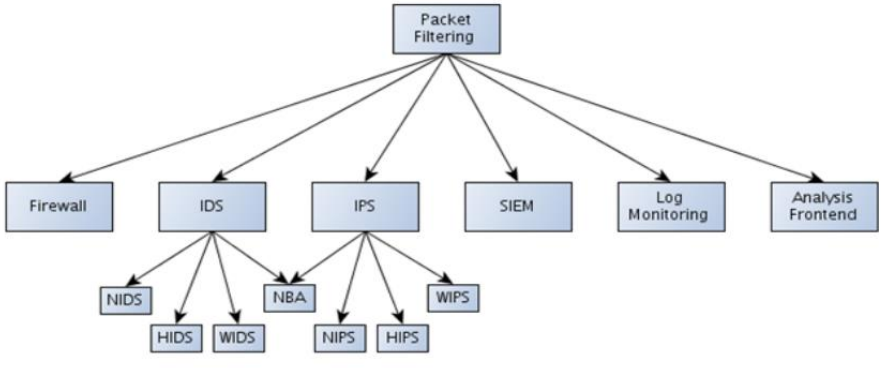
• Destination port: to which port the packet is going.

• Flags: URG, ACK, PSH, RST, SYN, FIN

Packet filtering looks at the source IP address, destination IP address, source port number, destination port number, flags and other information to decide whether some packet should be accepted or rejected. Usually, packet filtering is also smart enough to remember previous packets that are all analyzed together to decide if a packet is considered malicious and is rejected/dropped, or if it should be passed through.

Packet filter does not read the content of the packet or it cannot check the payload of the network packet; which implies that it cannot stop the application layer attack.

Packet Filtering Categories: An overview of packet filtering categories are shown in the below image



INTRUSION DETECTION SYSTEM(IDS):

An intrusion detection system can be software-based or hardware-based and is used to monitor network packets or system for malicious activity and perform a specific action if such activity is detected. Usually, if malicious activity is detected on the network, the source IP of the malicious traffic is blocked for a certain period of time, and all of the packets from that IP address will be rejected.

There are several types of intrusion detection systems:

• Network intrusion detection system (NIDS)

NIDS detects malicious activity by monitoring and examining network traffic. This type of IDS usually runs when packets enter a specific network on a special hardware component whose only job is to monitor and accept/reject packets from the Internet and let them into the local network. Example: Snort.

• A host-based intrusion detection system (HIDS)

HIDS detects malicious activity by monitoring and examining system calls, application logs, access control lists, etc. HIDS usually contains a software agent that needs to be installed on the operating system. Examples: Tripwire, OSSEC.

•A wireless intrusion detection system (WIDS)

WIDS monitors the wireless network for malicious behavior, which can be the number of packets sent in a time window, too many deauthentication packets, too many broadcast requests, etc. WIDS usually run on an AP (Access Point) and doesn't allow certain users to connect to it if malicious activity is detected.

• Network behavior analysis (NDA)

NDA monitors network traffic passively to detect unknown and unusual patterns that might be a threat. It should be used together with the firewall as well as other types of IDS systems.

INTRUSION PREVENTION SYSTEM(IPS):

The intrusion prevention system is basically an upgrade of the intrusion detection system. Where the IDS is used to detect and log the attack, the IPS is used to detect, block and log the attack. The IPS systems are able to prevent certain attacks while they are happening. There are multiple versions of the IPS systems, but we won't describe them in detail, since

they are the same as with IDS systems, with the exception that all of the types of IPS system also prevent the attack from continuing. The types of IPS systems are NIPS, HIPS, WIPS

SECURITY INFORMATION AND EVENT MANAGEMENT:

With SIEM we can monitor security alerts generated by various software or hardware solutions that are used for detecting malicious activity. SIEM consists of:

• SIM (Security Information Management): provides the analysis and reporting of the logged data.

• SEM (Security Event Management): provides monitoring and correlation of events.

A SIEM gathers information or data at a single point and provides a human-readable security report about the malicious behavior that is happening in our network. A SIEM solution must work in real time, so we can secure our network in a timely fashion. What would happen if we received a report about a security breach that is a month old, it wouldn't help us a lot since the attacker is probably long gone with all the data that he needed.

SIEM capabilities are as following:

• Data Aggregation: provides means to join data together from many sources: network, servers, databases, applications.

• Correlation: correlates data into meaningful sets to learn something new from it.

• Alerting: analysis of correlated events and alerting the recipients of detected security issues.

• Dashboards: provides means to present data in meaningful charts.

• Compliance: automatically gather all the needed data and produce reports.

• Retention: provides long-term storage of historical data for later analysis.

SIEM also implements log monitoring and analysis frontend, but we've nevertheless pointed them out as independent points in the above picture because other tools can be

available just for that. We can also write our own script that would take the logs and report some malicious activity. Log Monitoring and Analysis Frontend: It is an important part of the overall picture since this is the tool we use to look at the malicious activity that happened on our network. There are quite a few frontends available such as OSSIM, Sguil.

4.2 Windows and Linux Firewall:

we will see the details of the firewall in the different operating system such as Linux and windows and how it works. As both Windows and Linux are completely different operating systems, supports different file types, Linux is an open source and windows is a propriety one. Both operating systems can be used as a standalone machine as well as can be used for the server machine based on the requirements. But there is something common set of requirements for any user is to secure from the external threats. Many of the network administrators think that Linux has many advantages over windows, not just only freely available. But it is more stable than windows, less often crashing than windows. Easy configuration and less downtime required. Can be easily used for a file server, web server, email server, can be used in an intranet also as a router and firewall to help to connect to the network.

Windows Firewall:

Over the period of time windows operating system has grown much in providing its core functionality as an operating system. Windows Firewall was first included in Windows XP (back in 2001), and since then it has been improved in each new version of Windows. For every operating system, it is important to provide the core security infrastructure inbuilt within the operating system which handles implementing security protocols, enforcing security policies by providing dedicated firewall as software to monitor the network traffic. One of its roles is to block unauthorized access to your computer. The second role is to permit authorized data communications to and from your computer.

Firewall Functions in Windows Operating System:

Windows firewall with advanced security in windows server operating systems blocks unauthorized network traffic flowing into or out of a local device by providing host-based, two-way network traffic filtering. While the old Windows Firewall allowed you to configure only a single set of inbound and outbound rules (a profile), Windows Firewall

with Advanced Security includes three profiles (Domain, Private and Public), so you can apply the appropriate rules to each server based on its connection to the network.

• Domain networks. Networks at a workplace that are attached to a domain.

• Private networks. Networks at home or at work where you trust the people and devices on the network. When private networks are selected, network discovery is turned on but file and printer sharing is turned off.

• Guest or public networks. Networks in public places. This location keeps the computer from being visible to other computers. When a public network is the selected network location, network discovery and file and printer sharing are turned off.

You can also configure the following options for each of the three network profiles in advance windows firewall settings:

• Firewall State. You can turn the firewall on or off independently for each profile.

• Inbound Connections. You can block connections that do not match any active firewall rules (this is the default), block all connections regardless of inbound rule specifications, or allow inbound connections that do not match an active firewall rule.

• Outbound Connections. You can allow connections that do not match any active firewall rules (this is the default) or block outbound connections that do not match an active firewall rule.

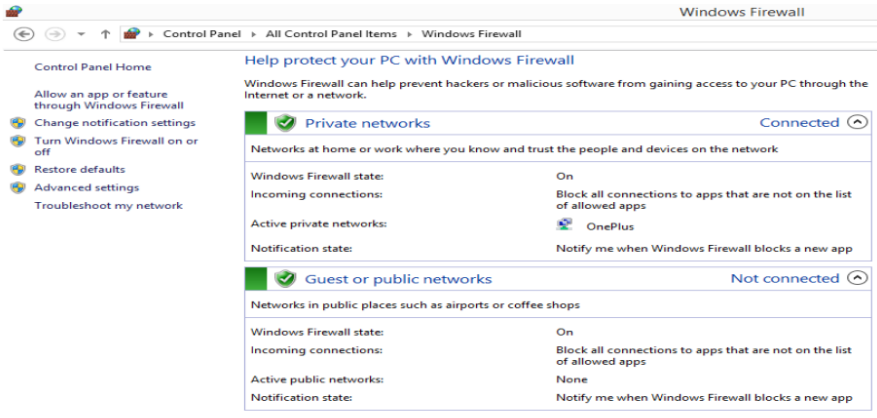
• Protected Network Connections. You can select the connections — for example, the Local Area Connection — that you want Windows Firewall to help protect.

• You can configure display notifications and unicast responses, and merge rules that are distributed through Group Policy.

• You can configure and enable logging.

• IPsec Settings. You can configure the default values for IPsec configuration.

Apart from the packet filtering, IP security windows also provide the functionality of the VPN(Virtual Private Network)



Virtual Private Network: A VPN, or Virtual Private Network, allows you to create a secure connection to another network over the Internet. VPNs can be used to access region-restricted websites, shield your browsing activity from getting trace back while on the public network. They originally were just a way to connect business networks together securely over the internet or allow you to access a business network from home. Most operating systems have integrated VPN support.

You can use a VPN to:

• Bypass geographic restrictions on websites or streaming audio and video.

• Protect yourself from snooping on untrustworthy Wi-Fi hotspots.

• Gain at least some anonymity online by hiding your true location.

• Protect yourself from being logged while torrenting

By default Windows Firewall is on and can be found as Goto Control Panel then goes to Windows Firewall. Click on the Windows Firewall and you will see the current status of the firewall and types of networks. Active connections if there are any. On the left side, there are several options to configure the default firewall setting to change it as per requirements.

On left side panel there in the above image, there is an option of Advance Setting on clicking that option will lead you to open another window of Windows Firewall with Advanced Security as shown below; Where you can set the inbound and outbound rules.

Linux Firewall:

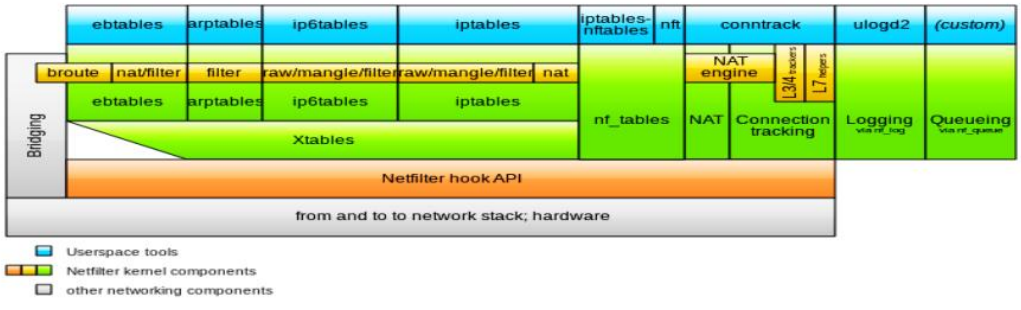
Before getting deep into the Linux Firewall we will go through some of the highlights of the Linux Operating System. Linux was created in 1991 by Linus Torvalds when he was an undergraduate student at the University of Helsinki in Finland. He has first created his own operating system based on Unix. After that nearly two decades Linux has become a fullfeatured operating system which is fast and reliable. Linux has got a solid reputation for efficiency and security. Linux is a multiuser operating system. Which means more than one user can log on into the system and can use the system at the same time; where mostly all versions of windows are the single-user system. Only one user at a time can log in a windows machine and can use it.

Linux has a very different way of using the file system, unlike windows. There is no concept of “C:/” Drive in Linux. Instead, Linux combines all drives and partitions into a single directory hierarchy. In Linux, one partition is designated as “root” partition. It is similar to the C:/ drive in the windows system. There are many distributions available based on the package manager which is either Debian based or RPM-based operating system in Linux. Though there are common components which are present in all different distributions which are Linux Kernal, administrative tools and packages.

An operating system such as Ubuntu, Lubuntu, are Debian based operating system which supports .deb packages. Another one is RPM-based package manager operating system such as Fedora, CentOS. Which supports .rpm based packages. Redhat is one operating which is the most stable version of RPM-based operating system and which doesn't come freely. Let us understand the security features of the Linux operating system.

Netfilter: Netfilter is a framework provided by Linux Kernal which allows networking operations to be implemented in the form of handlers. Netfilter supports different operations and functions for packet filtering, network address translation, a port translation which allows or rejects the network packets in the network.

The Netfilter framework included in the Linux kernel restricts incoming and outgoing network connections according to a set of rules that have been defined by the administrator. Several Linux distributions configure firewall rules by default and offer utilities for managing simple firewall configurations. You may also manage the firewall rules on any Linux system with the standard iptables and ip6tables command-line utilities. Use of iptables will only configure restrictions for IP version 4 connections and that you will need to use ip6tables to set up rules for IP version 6 as well.



Fedora, Red Hat, and SUSE automatically enable the firewall and supply their own graphical configuration utilities. You must manually configure and enable the firewall on Debian and Ubuntu systems. Current releases of Ubuntu include a command-line utility called ufw for firewall configuration.

Those Linux distributions that enable a firewall by default use a netfilter configuration that blocks connections from other systems. Any attempt by a remote system to access a service on a blocked port simply fails. This means that no other system may connect to an installed service unless you specifically choose to unblock the relevant port.

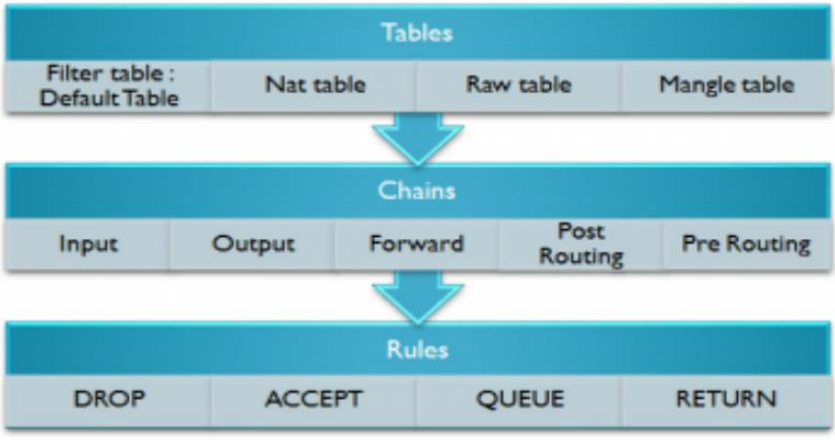
Let us try to understand the basic functionality such as NAT(network address translation), Port forwarding.

Network Address Translation: Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

Port Forwarding: Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

IPtables:IPtables which is an inbuilt firewall in Linux system. It is a user-based application for configuring the tables provided by the Linux kernel firewall. iptables is the default firewall installed with Red Hat, CentOS, Fedora distributions. Different modules and programs are used for different protocols such as iptables for IPv4, ip6tables for IPv6 and so on. It uses the concept of IP addresses, protocols (TCP, UDP, ICMP, etc) and ports. IPtables is a command line firewall that uses the concept of chains to handle the network traffic. It places the rules into chains, i.e., INPUT, OUTPUT, and FORWARD, which are checked against the network traffic. Decisions are made as to what to do with the packets based on these rules, i.e., whether the packet should be accepted or dropped. These actions are referred to as targets. DROP and ACCEPT are commonly used predefined targets used for dropping and accepting the packets, respectively.

IPtable architecture comprises groups of network packets, processing rules into tables and chains for processing the rules. Rules consist of matches to determine which packet the rule will apply to and the targets. They operate at the network layer.



Before you can configure rules with the iptables command, you have to understand a few concepts and Linux-specific terms

Tables: This is a default table that Linux firewall stores and maintains sets of rules. The main table is the filter table, where you define most rules that apply to incoming and outgoing traffic. The nat table contains rules that define how Linux performs NAT. The mangle table is used for advanced packet routing. Chains: Linux uses this term to refer to a set of rules that Linux applies when filtering network traffic. Here are the three main chains, each of which is part of the filter table: The three predefined chains in the filter table to which rules are added for processing IP packets are:

• INPUT: These are packets destined for the host computer.

• OUTPUT: These are packets originating from the host computer that leaves from the firewall.

• FORWARD: These packets are neither destined for nor originate from the host computer, but pass through (routed by) the host computer. This chain is used if you are using your computer as a router.

Let us see with the commands used on the Linux terminal, on how to work with iptables. Linux includes many different numbers of iptables commands. We will start with the basic syntax of the command-line options.

>>iptables [-t table] CMD [chain] [filter_match] [target]

Iptables commands must specify the table where the command will be applied, the command itself, the chain to which the command will belong, an expression that defines what type of traffic the filter will apply to, and what Linux should do with the packet. For example, to add a simple rule to the input chain of the filter table that would drop all ICMP traffic, your command-line would look something like this:

>>iptables -t filter -A INPUT –p icmp DROP

Above command tells the Linux system that, when the filter table's input chain receives the packet which uses ICMP protocol, send the packet to DROP target. Which simply means that to dump all ICMP protocol-related traffic.

Before moving to see more details we will first see the most commonly used iptables commands which are described in the below table.

Command	**Name**	**Description**
-A	Append	This command appends a rule to the end of a chain.
-I	Insert	This command inserts a rule to the beginning of a chain.
-D <chain><rule number>	Delete Rule	This command deletes a rule.
-L [<chain>]	List	This command lists all rules in a chain. If you don't specify a chain, the command lists the rules in all chains.

It is important to check the order of the commands used to prepare the rules. As Linux firewall. Once it matches the packet it no further checks for next defined rules. Because of this, iptables has the convenient -A command that appends commands to the end of the processing chain and the equally convenient -I command that adds commands to the beginning of the processing chain or a user-specified location. Now we will check the common iptables options available to prepare the rule.

-p protocol	Specifies the protocol. It can be TCP, UDP, ICMP or the protocol number which is listed in /etc/protocols.
-s source_address	Specifies source address of the packet. Also, specify the subnet mask along with the source address such as –s 192.168.1.2/24
-d destination_address	Specifies the destination address of the packet.
--source-port	Specifies the source port of a TCP or UDP packet.
--destination-port	It refers to the destination port of the TCP or UDP packet.
-i interface	Specifies the network interface for the incoming packet. For eg: -i eth0.
-o interface	Specifies an output interface on which packet is to be sent. For eg: -o eth1.

SELinux: Security-Enhanced Linux (SELinux) is a Linux kernel security module that integrated into the 2.6.x kernel using the Linux Security Modules (LSM)which provides a mechanism for supporting access control security policies, including mandatory access controls (MAC). It is a project of the United States National Security Agency (NSA) and the SELinux community. SELinux integration into Red Hat Enterprise Linux was a joint effort between the NSA and Red Hat. SELinux is also implemented as a standard feature in Centos/Fedora based distributions and widely deployed.

A Linux kernel integrating SELinux enforces mandatory access control policies that confine user programs and system services, as well as access to files and network resources. Limiting privilege to the minimum required to work eliminates the ability of these programs and daemons to cause harm if faulty or compromised (for example via buffer overflows or misconfigurations). This confinement mechanism operates independently of the traditional Linux (discretionary) access control mechanisms.

SELinux is set in three modes:

• Enforcing – SELinux security policy is enforced. If this is set SELinux is enabled and will try to enforce the SELinux policies strictly

• Permissive – SELinux prints warnings instead of enforcing. This setting will just give a warning when any SELinux policy setting is breached

• Disabled – No SELinux policy is loaded. This will totally disable SELinux policies.

SELinux is set in two levels:

• Targeted – Targeted processes are protected.

• Mls – Multi Level Security protection.

To check whether the SELinux is enabled or not in the Linux system you can use this below commands. You can use the CentOS or Fedora (RPM) based Linux distributions for the SELinux workings.

4.3 ATTACKS ON WIRELESS NETWORKS:

In today's time, the wireless network is present everywhere from home to data centers. They make life easy from the long and bulky cables and its related issues while ensuring the proper network connectivity with the internet to perform our everyday task in order to learn the wireless (In short Wi-Fi which came from wires fidelity) networks. It was first invented by AT&T in the Netherlands in 1991. We will also see the basics of the wireless networks first and it's different standards, security issues, and attacks and mitigation strategies. Also, we will learn about the SNORT tools which is basically and IDS/IPS tool used for securing and monitoring the network.

Wireless network in simple terms means the transformation of the information or power between two nodes without any kind of physical electrical conductor. Wireless technology uses radio waves for short and long-distance communication. There is a wide range of application of this wireless technology such as in telecommunication, satellite communications, mobiles, etc.

There are multiple types of wireless network exists which I am sure you will be aware by the names as Wide Area Network(WAN), Local Area Network(LAN), Mobile Adhoc Network(MANET). All these different types of networks are used for a different purpose but using wireless technology is at the core of all this. This network is a very popular choice for home users and from the small and medium size organization. There are three essential components of the wireless network that are radio signals, antenna, and router. The radio waves are the key which makes the Wi-Fi networking possible which are then converted to signals and picked by the WIFI receiver which is transmitted by the antenna. Then users are connected through the router for the communication.

The access point or router has a unique feature called as a beacon transmission, where it keeps on sending a signal on the wireless radio spectrum. This signal contains the network identification known as the service set identifier (SSID) and some trivial error correction information. The wireless receiver such as a laptop or any wireless device detects this signal in order to show it in the list of available wireless networks. It also detects whether or not the access point is using any security, and what level of security protocol, etc.

The access point or router contains TCP/IP stack which responds to ARP requests when a node tries to connect to it. Since wireless can allow multiple nodes at any instance, it is essential to have an authentication layer prior to starting the data transfer. It is the responsibility of the access point to ensure this security and monitor the packet transmission and data integrity.

Standards in Wireless Networks:

For the wireless networks, 802.11 is the working group from the Institute of Electrical and Electronics Engineers (IEEE) who defines the standard of operation for a specific technology. They are the group of expert members who works on it. There is multiple version of this. In each version, there is an improvement in the features of 802.11.

Standard	Frequency	Speeds	Interoperates with
802.11a	5 GHz	54 Mbps	None
802.11b	2.4 GHz	11 Mbps	None
802.11g	2.4 GHz	54 Mbps	802.11b
802.11n	2.4 / 5 GHz	100 Mbps	802.11b, 802.11g
802.11ac	5 GHz	1.3 Gpbs	802.11a, 802.11n

There are some common properties between all these standards there is also difference exist between these standards such as in terms of speed and speed and modulation Whether they are backward compatible or not. There is some difference in protocols and how the data is handled by different standards, but the attack and defense strategy will remain the same most of the time. The 802.11 standards will prescribe which frequencies these technologies work as well as which channel which also depends on the geographical locations. In the United States, There are 11 different channels available from 1 to 11 all are

separate, and they will not interfere with one another. The wireless network can work in two different modes such as Infrastructure and Ad-Hoc. There are some terminologies need to understand which are useful before moving forward and are related to understanding the wireless networks and communications.

SSID: Service Set Identifier is a human-readable name associated with an 802.11 wireless network. It is normally known as the network name.

BSSID: Basic Service Set Identifier uniquely identifies a specific access point and it is of the similar format as of the MAC address of the access point.

ESSID: Extended Service Set Identifier can essentially be thought of as a group of BSSID which shares the same layer of the network and same SSID.

As the wireless network doesn't have the in-built security mechanisms. Due to which a secure layer is built on top of the wireless network protocol stack. This is achieved by the encryption and authentication techniques such as WEP(Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). It is very important to secure the wireless networks as it can easily be intercepted. Let us now discuss in details regarding the attacks on the wireless networks. We will also in details regarding the steps of how to crack the wireless networks from the learning perspective which will help indirectly in how to design and implement the wireless network effectively with robust security features in an organization.

Also for the wireless network, the security comes from the selection of the security technique or the authentication method which is adopted. There are various different security technique which is available such as WEP (Wired Equivalent Privacy), WPA2(Wifi Protected Access II). WPA1 provides two different modes of operation which includes Personal or Pre-Shared Key(PSK) and Enterprise.

WEP: WEP is a very basic and original part of the 802.11 wireless standards. It provides encryption at layer 2 in an OSI layer. WEP utilizes the RC4 encryption algorithm to encrypt data and uses a shared key-system. It uses either 40 bit or 104 bit WEP key to encrypt data.

WPA2-PSK: It utilizes a shared key that is communicated to both sides access point and client before establishing a wireless connection. This key is then used for secure communication.

WPS2-Enterprise: It is also known as 802.1X which uses a RADIUS server for the authentication purpose. IT is achieved using EAP (Extensible Authentication Protocol)

Wireless Network Attack:

Any kind of wireless network attack is vulnerable and can cause the potential business impact. We will see several classifications which are described as below:

1.Access Control Attack: This attack tries to penetrate the wireless network or evading the access control mechanisms. War Driving: To discover wireless LAN network by listening to beacons using sniffing tools.

Rogue Access Point: Installing an unsecured or fake access point inside the firewall.

Ad Hoc Associations: Connecting directly to an unsecured station.

MAC Spoofing: To bypass the MAC filtering policy in access points attackers used to change the MAC address which matches to the access point MAC address whitelist. SMAC tool can help in changing the MAC address in windows.

RADIUS Cracking: RADIUS(Remote Authentication Dial In User Service) is a server which is used to authenticate client and server. This attack can be performed using a brute force attack to obtain the secret key

2. Confidentiality Attack: In these types of attacks attackers try to intercept the private information which is sent over a wireless network.

Eavesdropping: To capture the unprotected network traffic. Attackers mostly target the public wifi where the network usually does not have strong security measures.

WEP Key Cracking: To capture the network packets to recover the WEP key using active or passive methods.

Man In The Middle Attack: Attackers will try to capture the SSL connections in wireless networks and proxy them to web page logins to conduct the phishing attack. It can successfully complete this attack by first setting up the rogue access point and try to behave like a legitimate access point.

There are several steps involved to conduct such an attack which is listed below.

1. Select and target the access point and associated clients.

2. Identify the security protocol used such as WEP/WPA2 and crack the key.

3. Configure the wireless card as a rogue access point.

4. Use Airplay-ng to send de-authentication packets to target the host to disconnect from the network.

3. Integrity Attack: These types of attacks send the forged control and management or data frames over the wireless network to misguide them or to fulfill another attack.

Frame Injection: Specifically crafting and forging the 802.11 packets.

RADIUS Replay: To capture RADIUS accept and reject messages for later reply.

4. Authentication Attack: Attackers try to steal legitimate user identities and credentials to access private network and services.

VPN Login Cracking: To get the credentials using the brute force attacks on VPN authenticated protocols.

PSK Cracking: To crack and recover the password of WPA/WPA2-PSK from captured key handshake frames using dictionary attack tools.

5. Availability Attacks: These attacks stop the delivery of wireless services to legitimate users by denying them from accessing the WLAN resources.

Beacon Flood: Generating thousands of fake beacons to make it hard for stations to find a legitimate access point.

The next point we are going to see is to see how to crack the wireless network and get the encryption key. Also, we will see the process and tools usage which are mainly present in Kali Linux operating system.

But above all, it starts from understanding the basic cryptographic algorithm before starting to break it. As it is just built by using mathematical functions. Always under certain circumstances, weak implementation of the security mechanisms allows an attacker to reverse engineer it.

It applies to the wireless network protocols too. When a WEP encrypted packets are captured using Wireshark or any other similar tool, there is a field which is labeled as IV(Initialization Vector). Every packet has a different IV. IV is a 24-bit pseudo-random number which is there with every packet.

By passively capturing (stealth mode capture) the traffic to capture enough packets, WEP key can be cracked. As for 24-bit pseudo-random number, there are around 16 million unique IV's, which can easily be got by capturing the busy network traffic. So there are chances that multiple packets can have the same IV's.

Let us see the process.

1. Identify the target wireless network.

2. Passively monitor the encrypted packets between an access point and client using a sniffer tool.

3. Monitor ARP packets, as ARP packets are very small and having a unique size, also it would be easy for an attacker to reply for an ARP request and to start capturing.

4. Continue to send ARP request and get unique IV's.

5. Save around 50,000 encrypted packets to determine the WEP key.

6. Use the aircrack-ng program against the saved packets to obtain the WEP key. (aircrack-ng tools can be found pre-installed in Kali Linux). There are other tools which are present and used for wireless network attacks. Such as: Airmon-ng: Bash script to enable monitor mode on a wireless interface.

Airodump-ng: Wireless packet capturing tool designed for capturing packet for aircrack-ng. Airplay-ng: Packet Injection Tool for the wireless network to generate the traffic.

Aircrack-ng: It is a tool used for cracking key of WEP or WPA/WPA-PSK wireless network.

Various commands line utility or tools which are used for basic information gathering of wireless network which is listed below

iwlist wlan0 scanning

iwlist: Command line utility for identifying the wireless network

Kismet: Linux wireless network detection suite.

Netstumbler: Windows-based wireless network detection suite.

We have seen the basic overview of the WEP cracking, but now we will look inside each step in detail with commands. To start from identifying the NIC cards, scanning wireless networks in surroundings. The simplest way to identify the network wireless network cards in your system is using iwconfig. It will list out all network interfaces which are present in the system. There will be a wireless card which will be shown as wlan0 which will support the majority of all standards from (a,b,g, and n). Next step is to use an iwlist command which will help to gather initial information.

This command will give information such as ESSID, channel, frequency such information will be useful in later stages. There are several fields which will be seen in the output and use to perform the following tasks.

Encryption key: If this is set on, then the access point is using WEP encryption.

Channel: To see the current wireless channel for the specific BSSID.

Mode: If the mode is set to master, then it is an access point or else it is an Ad-Hoc Network.

Use the MAC address statically while performing such kind of testing. For cloning MAC address in Linux it is essential to bring down the interface first and to start again, this can be performed using the ipconfig command.

Let's begin with the process.

1. Identify the insure network using an iwlist command, which will consist of BSSID along with the channel.

2. Start the wireless card interface wlan0 into monitor mode using airmon-ng. For eg:

Start capturing the network traffic associated with the network using airodump-ng.

3.

-w DUMP: It will tell airodump to name all files in output to start with DUMP*.

-c : It tells airodump to stay connected on the channel specified, instead to jump In different channels.

--bssid: Just capture traffic related to target bssid.

Keep the window *>>airmon-ng start wlan0* open until we do not capture the sufficient numbers of packets. We have already seen that we need thousands of packets to gather enough number of IV to crack the WEP key. Goto the current working directory where you will see some pcap files

>>airodump-ng –w DUMP –c <channel> --bssid<MAC Address> mon0

which can be open and view with Wireshark. Now use aircrack-ng to see that pcap file to check how any number of packets are captured and how many numbers of unique IV are there. It will automatically tell whether we need more packets or we have enough number of the packet.

4.4 Application Inspection Tools:

The previous utilities in this chapter focused on support to find vulnerabilities over the web application through the script or some legitimate code. This section will covers the tool which identifies the SQL injection, logic flaws, XSS attack and many more. Also it focused on manual analysis of web application as well as traffic analysis over the web.

Zed Attack Proxy:

Zed Attack Proxy (ZAP) is an open source program or tool offered by OWASP (Open Web Application Security Project) for pen testing and discovers the vulnerabilities available in your web application or website.

ZAP provides to detect following kind of threats:

• SQL Injection

• Session management

• XSS

• Broken Access Control

• Security loophole in configuration file

• Sensitive data leak

• Inadequate protection

• Unsecure APIs

• Known vulnerabilities

ZAP provides various features as shown below:

• Active Scan

This is to discover known vulnerabilities against targeted attack.

• Alert

An alert is the prospective vulnerabilities with specified request. It has more than one alerted on per request. Alert have following risk like:

- High

- Medium

- Low

- Informational

- False Positive

It can be raised by ZAP components.

• API

Application Programming Interface (API) provides the functionality to configure ZAP programmatically. It supports HTML, XML and JSON formats.

• Authentication

ZAP handles various types of authentication that is used in web application like, Manual Authentication, Form Based Authentication, HTTP Authentication and Script Based Authentication.

• HTTP Session

Generally session is used to track the website. In ZAP, user can switch the user sessions on a website to create a new session instead of destroying the existing ones.

• Modes

ZAP has following modes:

- Safe: not dangerous
- Protected: potentially dangerous actions in URL

- Standard: you can do anything

- Attack: new nodes are actively scanned while it discovered

• MitM Proxy

MitM stands for Man-In-The-Middle proxy who allows you to check all the incoming requests and outgoing responses from the web application.

• Session Management

ZAP handles various kind of session management which will be used by website or web applications. It covers, Cookie based as well as HTTP authentication based session management.

• Tags It is a short information text which is associated with all requests. It can be manage by Manage Tags dialog.

The ZAP is installed by default in Kali Linux and the ZAP UI contains following elements:

(1) Menu Bar: Provide the various menus to perform the action on various tools.

(2) Standard Toolbar: This provides the button for easy access of tools.

(3) Tree view: It displays the websites tree and default context.

(4) Work area: This displays the various tabs like Quick Start, Request and Response, also allows editing the scripts.

(5) Information view: In this section you can see tabs like History, Search, Alerts and Output.

(6) Footer: In this section you can see the status of Alert such as High, Medium, and Low etc.

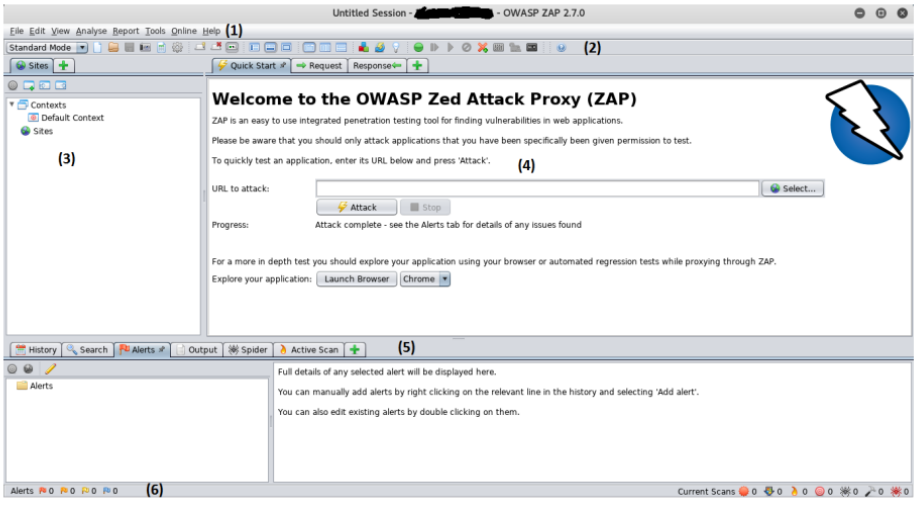
How to run Quick Start

Scan To run quick start scan:

(1) Start the ZAP and select Quick Start tab.

(2) In the URL to attack entry field, enter the URL or browse the URL by click on Select button.

(3) Click on Attack button.



The ZAP will process with its web crawler and scan each page of the web application or website. Then ZAP will perform the active scanner for attack on all the discovered web pages.

Damn vulnerable Web App (DVWA):

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. Before starting it must be ensure that the testing of DVWA should be done on an isolated host with either VMWare of Virtual Box, separated by a Host-only connection.

Some of the known vulnerabilities which DVWA contains as follows:

• Brute Force: HTTP Form Brute Force login page; used to test password brute force tools and show the insecurity of weak passwords.

• Command Execution: Executes commands on the underlying operating system.

• Cross Site Request Forgery (CSRF): Enables an'attacker' to change the applications admin password.

• File Inclusion: Allows an attacker to include remote/local files into the web application.

• SQL Injection: Enables an attacker to inject SQL statements into an HTTP form input box. DVWA includes Blind and Error based SQL injection.

• Insecure File Upload: Allows an attacker to upload malicious files on to the web server.

• Cross Site Scripting (XSS): An attacker can inject their own scripts into the web application/database. DVWA includes Reflected and Stored XSS.

• Easter eggs: Full path Disclosure, Authentication bypass and some others.

WARNING: THIS IS FOR EDUCATIONAL PURPOSES ONLY!

• Firstly install Xampp for windows. Then start the Xampp Control Panel from your desktop or from tray icon. Finally, start the MySQL and Apache services.

• Unpack the DVWA compressed folder into this location C:\xampp\htdocs\ dvwa.

• Now open your web-browser and type "localhost/dvwa" into the address bar. If any error occurs, this means that your PHP is not configured properly

• Go to the web-browser and type "localhost/dvwa/setup.php" and click on "Create Database" button. Then go to "localhost/dvwa/login.php" and provide the credential 'admin' as username and 'password' as password

Fig. DVWA Login

• Set the DVWA Security Level Low in "Script Security" as shown in following figure.

DVWA Security :It can be divided further into two parts, one is the security level and other is PHP IDS.

The security levels are named low, medium and high. By default the security level is set to high.

• High - It is used to compare the vulnerable source code to the secure source code.

• Medium - This security level is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application.

• Low - This security level is completely vulnerable and has no security at all. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

PHP-IDS is a popular PHP Intrusion Detection System (IDS) also known as a Web Application Firewall (WAF). PHP-IDS works by filtering any user supplied input against a blacklist of potentially malicious code. PHP-IDS is used in DVWA to serve as a live example of how WAFs can help improve security in web applications.

Web Goat: Web Goat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. You can install and practice with WebGoat.In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the Web Goat applications. It includes numerous exercises for topics ranging from Injection Flaws, over Cross-Site Scripting (XSS) to Denial of Service and many others. In the command-line of your liking, navigate to the location of the webgoat-container-7.1- exec.jar and start it:

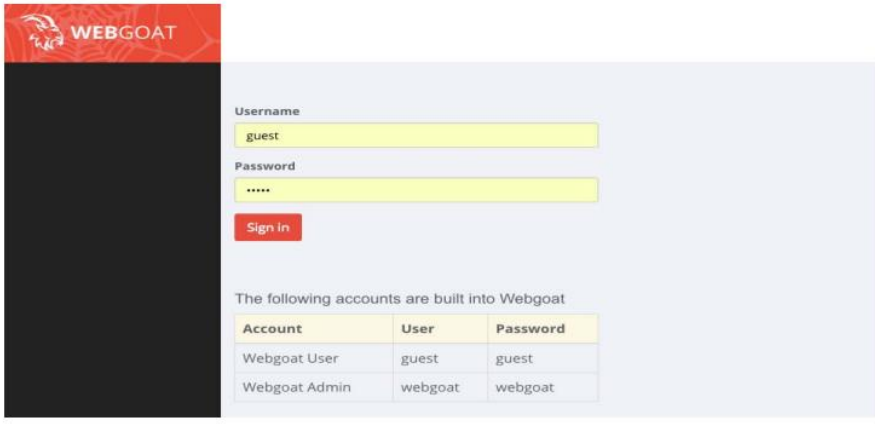
This will start a Webserver on port 8080.

You can access it via

```
java -jar webgoat-container-7.1-exec.jar
```

http://localhost:8080/WebGoat/ Login in Webgoat

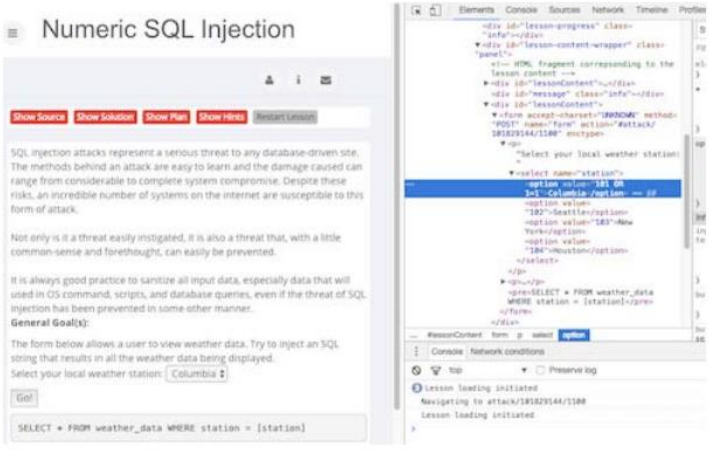
First, we log in using the guest account



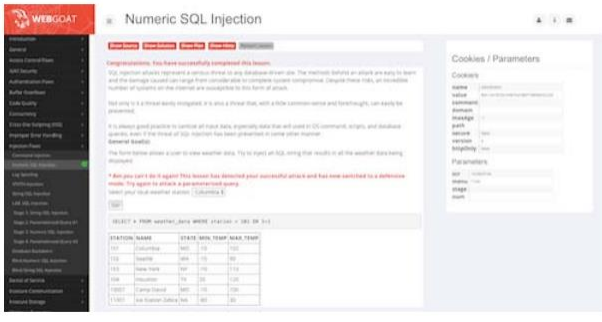
Then, we can have a look at the Tutorial with lots of helpful tips on how to get started with the WebGoat.

Alright, it's time for our first challenge! We will navigate to Injection Flaws and select the second entry Numeric SQL Injection from the slide out menu.

One possible solution to the Numeric SQL Injection exercise is to just open your browser dev-tools and change the value of the first option within the select field to 101 OR 1=1.



This will send the query SELECT * FROM weather data WHERE station = 101 OR 1=1 to the server, which is always true, hence returning all the stations.



Learning the basic techniques necessary to secure web applications is absolutely essential for professional web developers. The OWASP project and especially the WebGoat are great resources for doing exactly that. Especially in the field of web security, learning how to hack can be greatly beneficial for anyone aspiring to improve their skills in web security.

4.5 Password cracking and brute force tools:

In general, an attacker has two choices when trying to ascertain a password:

• Obtain a copy of the plaintext password or its encrypted hash and then use brute-force tools to guess what password produced the hash.

• Target a login prompt and try to guess a password. Password cracking is an old technique that is successful mostly because humans are not very good random-sequence generators. A Brute-force technique is a trial-and-error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard (DES) keys, through exhaustive effort (using brute-force) rather than employing intellectual strategies.

John the Ripper is one of the speedy password cracker, presently for many known operating systems like Windows, Unix, Mac, etc. Basically its main objective is to discover weak password in operating system. John the Ripper auto detects the encryption on the hashed data and compares it against a large plain-text file that contains popular passwords, hashing each password, and then stopping it when it finds a match.

It also includes its own wordlists of common passwords for 20+ languages. These wordlists provide John the Ripper with thousands of possible passwords from which it can generate the corresponding hash values to make a high value guess of the target password. Since most people choose easy-to-remember passwords, It is often very effective even with its out-of-the-box wordlists of passwords.

It is primarily a password cracker used during pen testing exercises that can help IT staff spot weak passwords and poor password policies.

Here is the list of encryption technologies found in John the Ripper:

• UNIX crypt

• Traditional DES-based • “bigcrypt”

• BSDI extended DES-based

• FreeBSD MD5-based (linux and Cisco IOS)

• OpenBSD Blowfish-based

• Kerberos/AFS

• Windows LM (DES-based)

• DES-based tripcodes

• SHA-crypt hashes (newer versions of Fedora and Ubuntu)

• SHA-crypt and SUNMD5 hashes (Solaris)

It is an open-source project, so you can download and compile the source on your own, download the executable binaries, or find it as part of a penetration testing package. The official website for John the Ripper is on https://www.openwall.com/john/. You can grab the source code and binaries there, and you can join the GitHub to contribute to the project. John the Ripper is available on Kali Linux as part of their password cracking metapackages.

Cracking password:

John the Ripper's primary modes to crack passwords are single crack mode, wordlist mode, and incremental. The single crack mode is the fastest and best mode if you have a full password file to crack. The wordlist mode compares the hash to a known list of potential password matches. The incremental mode is the most powerful and possibly won't complete. This is your classic brute force mode that tries every possible character combination until you have a possible result. The easiest way to try cracking a password is to let John the Ripper go through a series of common cracking modes. This command below tells it to try "simple" mode, then the default wordlists containing likely passwords, and then "incremental" mode.

```
.\john.exe passwordfile
```

You can also download different wordlists from the Internet, and you can create your own new wordlists for John the Ripper to use with the –wordlist parameter.

```
.\john.exe passwordfile–wordlist="wordlist.txt"
```

If you want to specify a cracking mode use the exact parameter for the mode.

```
.\john.exe --single passwordfile
.\john.exe --incremental passwordfile
```

When you want to see the list of passwords that you have cracked, use the –show parameter.

```
.\john.exe –show passwordfile
```

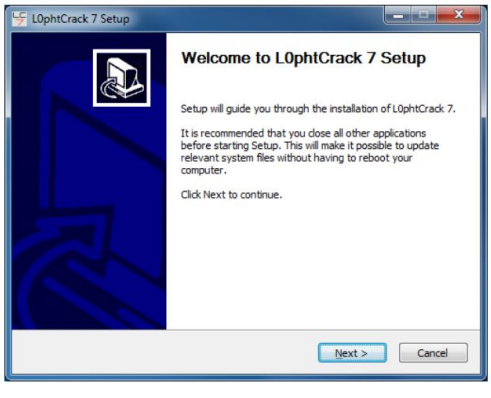
L0PHTCRACK:

L0phtCrack is known as best windows password auditing tool. It can be used by network/system administrator for auditing weak passwords and can also help a hacker to recover password from password hashes. To install L0phtCrack 7:

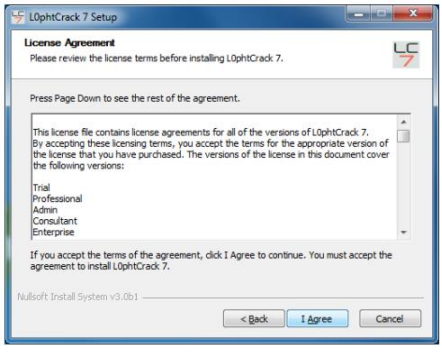
1. L0phtCrack 7 is distributed in a self-installing executable distribution file that can be downloaded for free at http://www.l0phtcrack.com/download.html.

2. Save the .exe file to your download directory.

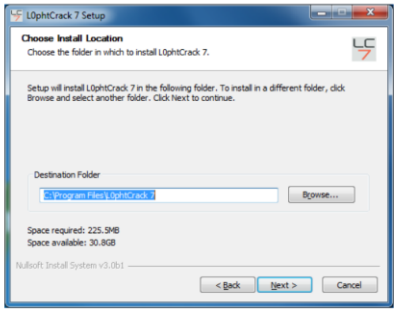
3. In the download directory, double click the lc7setup.exe file. The installer starts a standard installation process. At the Welcome screen, click Next.



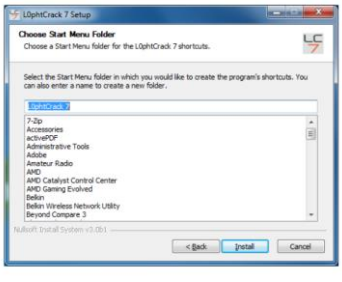
4. Read the License Agreement screen, then click I Agree to agree.



5. The installer installs L0phtCrack 7 in a default installation location: "C:\Program Files\L0phtCrack 7" or you may Browse to choose a different location. Click Next when ready.



6. A shortcut to the L0phtCrack 7 executable is installed in the Programs folder under the Start menu. The default folder name is L0phtCrack. You may choose a different name. Click Install when ready



7. L0phtCrack 7 is now installed on your system. You may now click the Start button, and go to the Programs folder to run L0phtCrack 7.

Importing password hashes: Approaches to importing password hashes differ depending on where the password resides on the computer and your ability to access them. L0phtCrack 7 can import password hashes directly from remote machines, from the local file system, from SAM, pwdump, or shadow files, and from Active Directory. Obtaining passwords over the network requires network access and administrator privileges to the target machine. To begin the import process select Import from the Passwords Menu Sidebar on the left hand side of the main screen. When Import is selected you will see the main window display the Import Mechanisms. When you select an Import Mechanism you will see the right side of the main window change to a dialog for the inputs required such as file and machine names. After you input the required filenames, hostnames and options for an Import Mechanism you will see the action buttons Run Import Immediately and Add Import To Queue ungray and become active. At this point you will likely press Run Import Immediately to perform the import action. Optionally you can press Add Import to Queue to build a queue.

Import from Local Machine: To import password hashes from a local machine, you must be logged in with administrator rights or have an administrator/password pair. The local machine import works regardless of whether passwords are stored in a SAM file or in an Active Directory. First, select Import from local Windows system. You can select to Keep Currently Imported Accounts if you are adding this import to accounts (hashes) you have already imported. If this option is not selected the import will overwrite any previously imported accounts. If you want to audit all system accounts, not just user accounts, you can select to Include Machine Accounts. Next, specify the credentials that will be used to access the password hashes. You can choose Use Logged-In User Credentials. If you previously saved credentials for the local machine you can Use Saved Credentials. You can also select Use Specific User Credentials. If specific user credentials is selected you need to specify Username, Password, and optionally a Domain. You can select Save These Credentials to save the username, password, and domain to the Windows protected store for use in future audits.

Import from Remote Machine: L0phtCrack 7 incorporates remote password hash retrieval, simplifying the process of obtaining password hashes, and reducing the need to use a third-party retrieval/dumping tool. To import from remote machines select either Import from Linux/BSD/Solaris/AIX system over SSH if your target system is Unix-like or select Import from remote Windows system if your target system is Windows. Credentials with Root or Administrator privileges are required. If a security tool or some other element in the network environment is preventing remote hash retrieval, then you may have to use a third

party tool to obtain the hashes and then follow the instructions for importing hashes from a pwdump file, SAM/System file (Windows), or shadow file (Unix).

PWDUMP:

The original pwdump program was written by Jeremy Allison in 1997 to demonstrate how to extract password hashes from the Windows Registry. Since then, other developers have created many versions of pwdump to keep up with various updates to Windows. But they all rely on extracting hashes from the Registry, SAMfile, or the lsass.exe process's memory space. The lsass.exe process handles the Local Security Subsystem Service; it's essentially responsible for authentication, which is why its memory contains the system's password hashes. All the pwdump variants may be found at www.openwall.com/passwords/microsoftwindows-nt-2000-xp-2003-vista-7. The Open wall site is also the home of John the Ripper, covered previously.

How to use PWDUMP:

The pwdump tools are simple to use. They require Administrator privileges, so you'll need to start the cmd.exe shell with Run As Administrator. The following example demonstrates pwdump6 on a 64-bit Windows system. The -x option is necessary to letpwdump6 know the target system is 64-bit. Otherwise, the process will hang without returning results. The -n option instructs pwdump6 to forego the search for password histories. The output may be passed to John the Ripper in order to start cracking hashes.

```
C:\pwdump6\PwDumpRelease> PwDump.exe -n -x localhostAdministrator:500:NO
PASSWORD*************:NO PASSWORD**********:::
Abs:1007:NO PASSWORD**************:2CxxxxxxxxxxxxxxxxxC01C591BC9:::
Guest:501:NO PASSWORD***********:NO PASSWORD**********************:::
Completed.
```

Note that neither the Administrator account nor the Guest account has a password set. This will be more common on home desktop systems because modern Windows systems encourage users to conduct their activities under their own account privileges and use the runas.exe or Run As Administrator commands to execute programs that require privileged access.

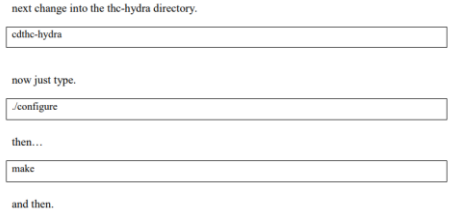
THC-HYDRA:

THC-Hydra (aka simply Hydra) easily surpasses the majority of brute-force tools available on the Internet for two reasons: it is fast, and it targets authentication mechanisms for several dozen protocols. Its source code and documentation are available from https://www.thc.org/thc-hydra/. The Hacker's Choice web site (https://www.thc.org) contains many security tools, although some of them have not been maintained for several years. THC (The Hackers Choice) created Hydra for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

If you are running Kali Linux you will already have a version of Hydra installed, for all other Debian based Linux operating systems download from the repository by using.

```
sudo apt-get install hydra
```

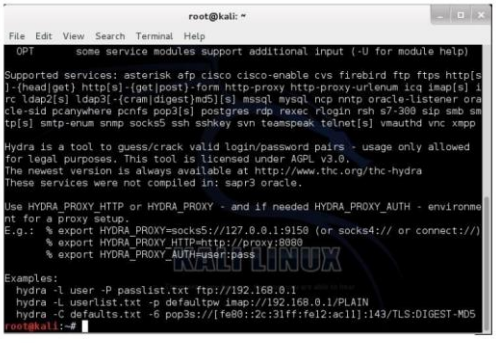
or you can download the latest version from THC's public GitHub development repository https://github.com/vanhauser-thc/thc-hydra Start by using git to clone the GitHub repository.



Hydra-GTK: Hydra GTK is a GUI front end for hydra, as this is a GUI for hydra you do have to have THC-hydra already installed. If you are running Kali Linux this will already be pre-installed for everyone.

Understand the hydra basics:

When we open Hydra, we are greeted with this help screen. Note the sample syntax at the bottom of the screen. Hydra's syntax is relatively simple and similar to other password cracking tools.



Let's take a look at it further.

```
hydra -l username -p passwordlist.txt target
```

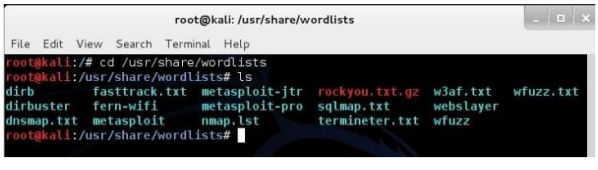
The username can be a single user name, such as "admin" or username list, passwordlist is usually any text file that contains potential passwords, and target can be an IP address and port, or it can be a specific web form field. Although you can use ANY password text file in Hydra, Kali has several built in. Let's change directories to /usr/share/wordlists:

```
kali> cd /usr/share/wordlists
```

Then list the contents of that directory:

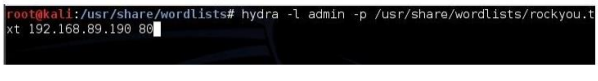
```
kali>ls
```

You can see below, Kali has many word lists built in. You can use any of these or any word list you download from the web as long as it was created in Linux and is in the .txt format.



Use Hydra to Crack Passwords

In the example below, I am using Hydra to try to crack the "admin" password using the "rockyou.txt" wordlist at 192.168.89.190 on port 80.



4.6 Web Attacks:

Technology growth on the Web has changed the way businesses and consumers communicate and interact with each other. The Web has become a staple for information sharing and commercial transactions. At the same time it has also become complex, without boundaries and immediate in its nature. Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

A single Web page today can be comprised of information from many simultaneous sources from around the world. It only takes one of these sources to be compromised in order for a new Web attack to be quickly propagated and delivered to many unsuspecting Web users. The ubiquity and complexity, compounded with holesin the infrastructure, have made the Web vulnerable to attack.

Of all the software in use, browsers are the most exposed. They are constantly connecting to the outside world, and frequently interacting with websites and applications that cybercriminals have infected with malware. Browsers are powerful, data-rich tools that if compromised, can provide an attacker with a vast amount of information about you, including your personal address, phone- number, credit card data, emails, IDs, passwords, browsing history, bookmarks etc.

Browsers are also perfect instruments for cybercriminals to establish a foothold on your device, your personal network, and your business systems. Browsers rely on a number of third-party plug-ins like JavaScript, Flash, and ActiveX to perform various tasks. However, these plug-ins often come with security flaws that cybercriminals exploit to get access to your systems. These vulnerabilities allow attackers to wreak havoc by, for example, installing ransomware, exfiltrating data, and stealing intellectual property. During the past year or so, we've seen a sharp increase in web threats that are specifically designed to leverage browser-based vulnerabilities.

This increase in popularity is not only because browsers are strategically desirable as hacking targets, but because browser-based web threats are difficult to detect. Most malware detection and prevention technologies work by examining files such as downloads or attachments. However, browser-based threats don't necessarily use files, so conventional security controls have nothing to analyse. Unless organizations implement advanced tools that don't rely on analysing files, browser-based attacks will likely go undetected.

As an example of how a browser-based attack works, consider a scenario where a Windows user visits a seemingly benign but now malicious website, possibly one he or she has visited before, or as the result of an enticing email. As soon as a connection occurs, the user's browser begins interacting with the site. Assuming the system is using JavaScript, which according to research firms like Web Technology Surveys, 94% of all websites do and over 90% of browsers have it enabled, the browser will immediately download and start executing JavaScript files from the malicious website. The JavaScript can harbour malicious code that's capable of capturing the victim's data, altering it, and injecting new or different data into their web applications—all in the background and invisible to the user. For instance, one method malware authors use to accomplish this is by embedding an obfuscated Adobe Flash file within the JavaScript. Flash is frequently used due to its seemingly never-ending set of vulnerabilities. The following is representative of what typically occurs:

• The Flash code invokes PowerShell, a powerful OS tool that can perform administrative operations and exists on every Windows machine.

• Flash feeds instructions to PowerShell through its command line interface.

• PowerShell connects to a stealth command and control server owned by the attackers.

• The command and control server downloads a malicious PowerShell script to the victim's device that captures or finds sensitive data and sends it back to the attacker.

• After the attacker has met his objectives, the JavaScript, Flash, and PowerShell scripts are wiped from memory, leaving essentially no trace of the breach.

The MarioNet attack is a browser-based attack; it opens the door for assembling giant botnets from users' browsers. These botnets can be used for in-browser crypto-mining (cryptojacking), DDoS attacks, malicious files hosting/sharing, distributed password cracking, creating proxy networks, advertising click-fraud, and traffic stats boosting, researchers said. Moreover, MarioNet can survive after users close the browser tab or move away from the website hosting the malicious code.

Web Attacks targeting Attacks: Cyber criminals often go after your enterprise data by preying on your end users. Here are some of the most current exploits to watch for. Every day, criminals devise new malware and social engineering attacks that target what has become an organization's weakest link: end users and their Web-connected devices. Here

are the most common attack methods and social engineering techniques, and ideas on how to stop these attacks before they infect end user devices and work their way into your corporate data.

Drive-by downloads: are a central part of many of the most sophisticated Web attacks that criminals perpetrate against online users. They are so dangerous because they require no user action to download malicious content onto an endpoint. What's more, these attacks are often unleashed from legitimate sites. Drive-by downloads are typically deployed by hackers who have taken advantage of Web vulnerabilities such as SQL injection that can be exploited to "allow attackers to change the content of a website," says Chris Wysopal, CTO at the app security testing company Veracode. Once implanted on a site, drive-by downloads typically take advantage of browser vulnerabilities to automatically download anything from full-fledged viruses to less detectable downloader apps that will trick the user into eventually loading malware onto the machine via a button press or click.

Clickjacking: If the attacker requires extra interaction from the user to load malware, this will be accomplished through an attack called "clickjacking." The purpose of this attack is to open the target website in an invisible frame and get the user to click somewhere in the frame when they don't even know they're clicking in that website," says Ari Elias-Bachrach, application security consultant and trainer for security consultancy Defensium. "In this way, you can trick the user into making a mouse click that does something [malicious] on the website. A common example is offering a bogus pop-up window made to look like a legitimate plugin update or antivirus alert, such as a Microsoft Security Essentials window that says you have a few viruses and should push a button to clean them. "The pop-up itself is not harmful, but if you click the button, you open the gate to infect your machine," says Rick Doten, chief information security officer for DMI, an enterprise mobility company.

Plugin and script Enabled Attacks:

Not only do attackers look for vulnerabilities within the browser itself, they also frequently ferret out bugs in browser plug-ins and scripting programming to help them carry out driveby downloads and clickjacking attacks. Since these attacks rely on known vulnerabilities, "make sure users keep browsers and browser plug-ins updated to the latest versions by enabling auto-update functions," says Wolfgang Kandek, CTO of vulnerability management firm Qualys. In some cases, it may also make sense to turn off scripting within the browser and other susceptible programs, such as Adobe Reader. Similarly, uninstalling

certain problematic plug-ins can reduce the attack surface within susceptible user bases. But you'll still need to put controls in place and train users not to undo the work.

Advanced Phising Attacks:

While phishing attacks are typically associated with email, most are perpetrated via links to malicious content on the Web, whether a simple password capture form used in traditional phish attempts or a malicious drive-by download in more advanced targeted attacks. Phishing attacks are designed to trick users into thinking they are a link from an organization or person they know, making people feel safe enough to click or divulge information they otherwise wouldn't. Many corporate security training programs have helped users spot the most obvious first-generation phishing attempts, which were designed to steal credentials such as banking passwords. But attackers are getting more crafty.

Social(Engineering)Networks:

Millions of people sharing information on social networking sites such as Facebook, Twitter, LinkedIn and Google+ creates "an ideal attack bed for someone who wants to socially engineer a target individual, group of individuals or an organization as a whole," says Joe DeSantis, manager of incident response at security consultancy SecureState. If people don't configure their privacy settings very stringently, attackers can simply troll their pages to dig up information about the target and then hone a particularly effective spear phishing email. Or attackers can pose as friends or family to "friend" a target -- or a friend of the target -- to gain that intelligence. They can also use a social networking connection to directly send targets malicious links on their walls or Twitter feeds.

Obtaining User or Website data:

The value of web data is increasing in every industry from retail competitive price monitoring to alternative data for investment research. Getting that data from a website is vital to the success of your business. Web scrapers automatically collect information and data that’s usually only accessible by visiting a website in a browser. By doing this autonomously, web scraping scripts open up a world of possibilities in data mining, data analysis, statistical analysis, and much more.

Why Web scrapping is Useful:

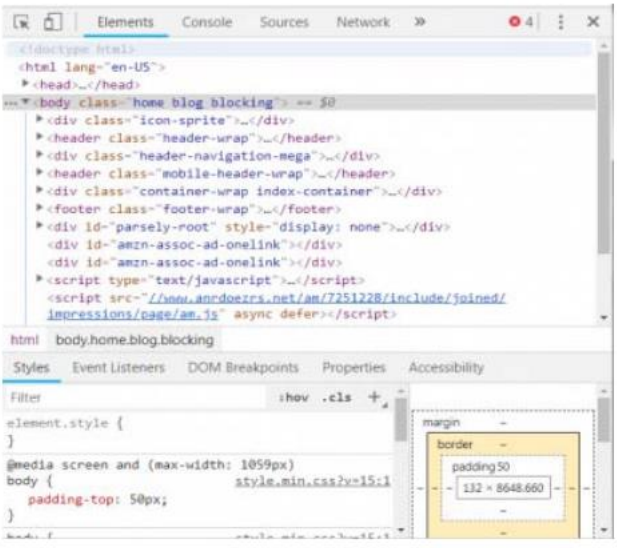
We live in a day and age where information is more readily available than any other time. The infrastructure in place used to deliver these very words you are reading is a conduit to more knowledge, opinion, and news than has ever been accessible to people in the history of people. So much so, in fact, that the smartest person's brain, enhanced to 100% efficiency (someone should make a movie about that), would still not be able to hold 1/1000th of the data stored on the internet in the United States alone. As our eyes and brains can't really handle all of this information, web scraping has emerged as a useful method for gathering data programmatically from the internet. Web scraping is the abstract term to define the act of extracting data from websites in order to save it locally. Think of a type of data and you can probably collect it by scraping the web. Real estate listings, sports data, email addresses of businesses in your area, and even the lyrics from your favourite artist can all be sought out and saved by writing a small script.

How Does a browser get web data:

First, your browser will take the URL you entered or clicked on and form a "request" to send to a server. The server will then process the request and send a response back. The server's response contains the HTML, JavaScript, CSS, JSON, and other data needed to allow your web browser to form a web page for your viewing pleasure.

Inspecting Web Elements:

Modern browsers allow us some details regarding this process. In Google Chrome on Windows you can press Ctrl + Shift + I or right click and select Inspect. The window will then present a screen that looks like the following.



Other types of responses:

Additionally, servers can return data objects as a response to a GET request, instead of just HTML for the web page to render. A website's Application Programming Interface (or API) typically utilizes this type of exchange. Scraping frameworks are available in Python, JavaScript, Node, and other languages. One of the easiest ways to begin scraping is by using Python and Beautiful Soup.

Email Attacks:

Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks to deliver malware, lure victims to malicious websites, and steal logon credentials, and organizations everywhere need to understand these threats and how to implement effective safeguards. Many people rely on the Internet for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Email is a universal service used by over a billion people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations. Malicious email authors are clever and relentless, and they are constantly developing new or at least different ways to deceive and attack us. Although the malicious payloads found

in email-based attacks frequently change, the vast majority of cybercriminals use basic strategies:

Malicious attachments: Emails often include dangerous attachments that install keyloggers, ransomware, and other malware when opened by the victim. Links to malicious web pages: Contained in either an attachment or in the body of the email, links to dangerous web pages also account for a significant number of data breaches.

Below are some of the most common types of Attacks:

Phishing: Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information. Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person. The criminal researches the target's interests before sending the email.

Whaling: Whaling is a phishing attack that targets high profile targets within an organization such as senior executives. Additional targets include politicians or celebrities.

Pharming: Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they connected to a legitimate site.

Adware: Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyse user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.

Spam: Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

4.7 Cyber Crime:

After studying this unit student should be able to:

• Types of Cybercrime,

• Hacking,

• Cyberspace and Criminal Behaviour,

• Clarification of Terms,

• Traditional Problems Associated with Computer Crime,

• Introduction to Incident Response,

• Digital Forensics,

• Computer Language,

• Network Language,

• Realms of the Cyber world

"Cyber-Crime" Computer crime, or cybercrime, is crime that involves a computer and a network. Cyber-crime involves activities like raiding bank accounts and stealing information from companies. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes are offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet chat rooms, emails, SMS/MMS, notice boards and groups and mobile phones such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare

Types of Cyber café:

• Crime against individual

• Crime against property

• Crime against organization

• Crime against society

Crimes against individuals email spoofing a spoofing mail is the formation of email messages by impersonating correspondent. Email spamming spam is a message also called as junk mail sent with a web link or business proposal clicking on this link or replying to commercial offer sent to a phishing website or set up a mall where in your workstation the sender's of this electronic email are always unidentified. Crime against Property credit card fraud online fraud and cheating are most money spinning trades those are raising nowadays in the cyberspace it may have diverse forms some of the cases of online fraud and cheating that are uncovered are those referred to credit-card offences contractual crimes offering employment etc. Intellectual property crimes intellectual property involves a list of Rights any illegal act due to which the owner is deprived entirely or part of the his human rights. It is a crime the very common form of IPRabuse may be known to be software piracy, copyright infringement, trademark and service mark violation theft of a computer source code. The Hyderabad Court has in a landmark judgment has convicted three person and sentenced them to six months custody and fine off rupees 50,000 each forum authorized copying and sell of pirated software. Against Organization unauthorized access this is generally denoted to and hacking the intent law has however given a different connotation to the term hacking so we will not use the term unauthorized access interchangeably with the term hacking to prevent misperception. As the term used in the IT Act 2000 of India is much wider than hacking. Denial of service attack in simple words denial of service referred the act by which a user of any website or service denied to use the service or web site. In this category of cyber-crime offenders in the web server of the websites and flow a large number of requests to that server this causes the use of maximum bandwidth of the website and it goes slow down not available for sometimes.

Virus attacks a computer virus is a type of malware that when executed replicates by implanting the replicas of it probably altered into other computer programs data files or the boot sector of the hard drive. When this reproduction proceeds the affected zones are then said to be infected. Viruses frequently do certain type of dangerous activity on infected

hosts such as stealing hard disk space or CPU time retrieving, private information corrupting, data displaying radical often emails on the user's display spamming their links or logging their keystrokes. However not all viruses can have a damaging consignment or effort to hide themselves the describing features of viruses is that they are self-duplicating computer programs which mount themselves without the users approval. On the other hand computer worm is a separate more than program that copies itself in order to disperse to other computers frequently.

It uses a computer network to spread itself depend on security failures on the aim computer to allow it. Unlike a computer virus it does not require to join itself to a prevailing program email bombing. IN email bombing user is sending vast numbers of emails to target address and due to this that email address or mail server crashed. It feels like denial of service impression it says that spamming is a variant of male bonding salami attack. A salami attack is when minor attacks make up a major attack which becomes untraceable because of its nature.

It is also called a salami slicing though salami slicing is frequently used to transport unlawful activities it is only a plan for gaining and benefit over time by collecting it in small increments so it can be used in perfectly legal ways as well the attacker uses an online database to seize the information of customers.i.e. bank credit card details deducted very little amount from every account above a period of time the customers remain unaware of the slicing and hence no complaint is launched thus keeping the hacker away from detection.

Logic Bomb: A logic bomb is a piece of code intentionally inserted into a software system that will initiate mischievous features under definite conditions, for example a programmer may hide a part of code that starts initiating deleting files such as salary database. Malicious programs such as viruses and worms often contain logic bombs that execute a certain payload at a predefined time or when some other condition meets. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their whole systems on particular dates such as, April fool's Day. Trojans that trigger on certain dates are frequently known as time bomb Trojan horse a Trojan horse or Trojan in computing is anon-self-duplicating kind of malware program comprising malicious code that when implemented carries out actions determined by the nature of the Trojan Usually causing damage of stealing of data and likely system damage.

The term is derived from the tale of the wooden horse used to trick defenders of Troy into taking concealed warriors into their city in ancient Greece because computer trojans

often hire a form of social engineering representing themselves as routine valuable or interesting in order to encourage victims to install them on the computers. A Trojan generally acts as a backdoor communicating a supervisor that can have unlawful access to the affected computer. The Trojans exit are not themselves easily noticeable but if they carry out substantial computing or communications activity may cause the computer to run noticeably slow data.

Hacking:

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers. They just hack to see what they can hack and what they can't hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information. The knowledge that malicious hacker's gain and the ego that comes with that knowledge are like an addiction. Some hackers want to make your life miserable, and others simply want to be famous. Some common motives of malicious hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure. Many hackers say they do not hack to harm or profit through their bad activities, which helps them justify their work. They often do not look for money full of pocket. Just proving a point is often a good enough reward for them.

Steps Performed By hackers

1) Reconnaissance

• Performing Reconnaissance

2) Scanning

• Scanning and Enumeration

3) Gaining Access

4) Maintaining Access

• Maintaining access and Placing Backdoors

5) Clearing Tracks

• Covering tracks or Clearing Logs

Phase I: Reconnaissance

Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.

Phase II: Scanning and Enumeration

Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

Phase III: Gaining Access

This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the hacker world as owning the system. During a real security breach it would be this stage where the hacker can utilize simple techniques to cause irreparable damage to the target system.

Phase IV: Maintaining Access

Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans. The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

Phase V: Clearing Tracks In this phase

once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

The Indian IT Act, 2000 defines and punishes “Hacking” as follows: Hacking with computer systems

• Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes any information residing in computer resources.

• “Whoever commits hacking shall be punished with imprisonment up to three years, with fine which may extend up to 2 lakh rupees or both”

• Hacking has been very widely defined in the law of Information Technology, which is much wider than the concept of “hacking” as understood in common.i.e. “Breaking into computer systems”.

• “Destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means”.

Cyberspace and criminal behavior:

Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be thought of as the interconnection of human beings through computers and telecommunication, without regard to physical geography.

The word became popular in the 1990s when the uses of the Internet, networking, and digital communication were all growing dramatically, and the term "cyberspace" was able to represent the many new ideas and phenomena that were emerging. There are no shared definitions of cyberspace at the scientific level and every government uses a different definition. Cyberspace is the national environment in which digitized information is communicated over computer networks.” -Dictionary of Military and Associated A global domain within the information environment consisting of inter dependent network of

information technology infrastructures including the Internet, telecommunications networks, computer systems & and embedded processors and controllers.

Cyber security is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. Cyber security standards are the specifications which enable organizations to practice safe security techniques to minimize the number of successful cyber-attacks. Cyber security refers to the technologies and processes designed to protect computers, networks and data from unauthorized access, vulnerabilities and attacks delivered via the Internet by cyber criminals. Though, cyber security is important for cyberspace.

Traditional Problems Associated with Computer Crime Individuals seeking a crime has always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves no specialist users (e.g., child pornographers, narcotics traffickers, and predators). In fact, the earliest computer crimes were characterized as no technological. Theft of computer components and software piracy were particular favourites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crimes came later.

Although the advent of technology has vastly changed the modus operandi of certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty. Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations.

At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do

so.Physicality and Jurisdictional Concerns The physical environment that breeds computer crime is far different from traditional venues. In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents. For example, what forensic tools are available for identifying entry points in data breaking and entering? Certainly, seasoned investigators recognize the utility of prymark analysis in home burglaries.

Cyberspace and criminal behavior:

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Associate Professor at the Sorbonne Business School), technical expertise and accessibility no longer act as barriers to entry into cybercrime. Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc. By comparison, a mail software-as-a-service is a scalable, inexpensive, bulk, and transactional e-mail-sending service for marketing purposes and could be easily set up for spam. Jean-Loup Richet explains that cloud computing could be helpful for a cybercriminal as a way to leverage his attack – brute-forcing a password, improve the reach of a botnet, or facilitating a spamming campaign. Cyberspace has become an ideal place for criminals to remain anonymous while preying on victims. As the number of cyberspace users increase, so do the opportunities for exploitation and the need of protecting computers, networks, digital applications, programs and data (i.e., sensitive business and personal information) from unintended or unauthorized access, change or destruction. The Department of Homeland Security (DHS) affirms that there is a range of traditional crimes now being perpetrated through cyberspace.

Criminals hide in the net to perpetrate quite effortlessly crimes that, in earlier times, required physical travel and a more direct involvement. As the cyberspace is recognized as a critical domain for conducting everyday distant operations, unfortunately, it has also become a ground for cyber-terrorism and menaces of cyber war attacks. Cyber terrorists may use various forms of computer-related abuse tactics (e.g., hacking, cracking, phishing, spamming) to accomplish their personal or politically motivated goals. However, countries and governments are not the only targets of cyber criminals. Businesses are not safe either; vital corporate data and industrial secrets can be stolen from adversaries, for example, with

cyber espionage; in the past, some attempts have come from countries including China and Russia. In fact, the financial sector is one of the most targeted in recent times and has been the theater of attacks that have often captured the interest of the media. Recent news, for example, report of a large operation conducted in Europe against a multinational organization operating in Italy, Spain, Poland, Belgium and the UK. Cyber criminals were able to infiltrate malware in the systems of some large European companies and route money to bank accounts they controlled: a $6.8 million business. EC3, the Europol's European Cybercrime Centre, discovered that the organization was operating from Cameroon, Nigeria and Spain through an impressively efficient money laundering system. Cybercrime has really no borders and boundaries. In recent years, "information warfare," a new form of terrorism, has captured the attention of information security specialists; terrorists might tamper with computers to commit information-based threats to nations, to businesses, and to individuals.

Economic Impact of cyber crime:

Cyberspace is vulnerable to a wide range of risks, affirms the DHS Cyber Security Division, saying it brings substantial human and economic consequences. All computers users are at risk of Internet crime. According to the Norton Cybercrime Report for 2011, "1m+ adults become cybercrime victims every day." As per a study jointly conducted by McAfee and the Center for Strategic and International Studies in June 2014 (Net Losses: Estimating the Global Cost of Cybercrime), computer-related crimes may cause as much as $400 billion in losses annually, while cyberattack-related losses could be as much as 575 billion. However, arriving at an estimate for the financial losses suffered because of cybercrime is difficult because many instances simply go unreported. Cybercrime can mean incredible losses for businesses, but is a great deal for perpetrators. Trustwave's "2015 Global Security Report" estimated that the average cybercriminal has a 1,425 percent return-on-investment (ROI). These figures can definitely explain the proliferation of attacks.

Cybercrime trends:

In a world where information and communications technology (ICT) that provides the means so people can work with each other electronically in a digital form over great distances, cyber threats are of great concern. Though it is difficult to keep up with the changes as ICT is constantly evolving, an understanding of the concepts and technologies for achieving confidentiality, integrity, authenticity, and privacy protection for information processed across networks is paramount. Cybercriminals often use 'bots' – a network of software robots – to infect and control networks and control them remotely for malicious

purposes. From phishing and devious social engineering efforts to using spyware tactics, an invader can carry out an attack on specific targets, exploiting zero-day vulnerabilities, upload malware on certain platforms, if not collect information and gain access to systems for other purposes. In fact, botnets are often used to spread remote code execution malware.

Coming familiar with botnet cyber threats (i.e., how they work and spread malicious code infecting each host and then propagate into the network) is vital to preventing the botnets from the beginning. Examples of botnet attacks are easy to find. The Game Over Zeus botnet (a sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects) that occurred in 2014, according to the FBI, it was believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world.

As per the FBI, "Unlike earlier Zeus variants, Game Over has a decentralized, peer-to-peer command and control infrastructure rather than centralized points of origin, which means that instructions to the infected computers can come from any of the infected computers, making a takedown of the botnet more difficult. But not impossible." The growth of the use of cloud computing and the Internet of Things (IoT) is contributing greatly to the problem. According to Security Expert and bestselling author, Marc Goodman, in fact, the number of devices connected through the Internet is growing exponentially, and security is an issue: the average IoT, he estimates, has over 20 security vulnerabilities, a number that poses serious concerns.

Another alarming trend, according to Goodman, is the new cybercriminals' profile, who, in most cases, are no longer teenagers looking for glory, but consummate professionals that choose cybercrime as a profession and can sell services. The new breed of malicious hackers is made of more sophisticated criminals who can actually operate within highly organized establishments.

In addition to more specialized hackers, computer software is increasingly been used to perpetrate cybercrime. Crimeware-as-a-service is a new option for criminals without particular technical skills who can carry out their agenda by using off-the-shelves products designed for that purpose. Defending ourselves from this new, decentralized, and pervasive cybercrime is a daunting task.

There is no arguing, "Cybercrime is a global problem." With the ability to connect anything and everything to the Web, cybercriminals exploit the inherent connectivity when

and where they like. When it comes to Internet crime, there are all sorts of law-breaking offenses committed that range from identity theft and fraud to unethical hacking, illegal downloading of media, online harassment (e.g., cyberstalking, cyberbullying, to include sexting, child soliciting and abuse), among others. Recurring crimes include sending malicious software to disrupt a network or gain access to a system with the motive to steal sensitive information or data, if not to cause damage to system software. Laws and regulations vary across the country. (See, for example, U.S. state-specific computer crime laws.

Users are called upon to be the first line of defence and help reduce cyber risks and data compromised by hackers through proper use of their computer, mobile phone and other devices. A Trustwave study showed how 81% of victims they surveyed did not detect breaches in their systems but were notified by external entities. The Verizon's 2015 Data Breach Investigations Report further found that, in 66% of the cases they analyzed, it actually took a few months to discover the crime. Situational awareness, then, is one of the key areas of cyber defense and is invaluable when coupled with monitoring and malware analysis from IDS alerts and log files gathered by those in the field. In 60% of the cases, it only took a few minutes for cybercriminals to cause damage to the organizations they attacked, so it is important that everyone in an organization is always looking for anything suspicious in the way their systems behave. Even DHS has created an on going cybersecurity awareness campaign Stop.Think.Connect. launched on October 4, 2010 to help people to understand the risks that come with being online.

Despite IDS/IPS technologies being deployed, only a small percentage of IT decision makers are truly confident that these devices alone will work against a cyber-threat; therefore, they are still seeking alternative solutions, mentioned Tara Seals, US/North America News Reporter, Info security Magazine, in a recent post. Seals explains also the importance of perimeter-based cyber-security models – characterized by a multi-level approach involving firewalls, anti-virus software and powerful analytic tools searching for anomalies in network behaviour across the enterprise – to protect against threats (or to reduce the damage they can cause), as they continue to evolve rapidly.

Cyberspaces and criminal behavior:

Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.4 Although originally coined in 1984 by science fiction writer William Gibson, it is hardly a new concept. In fact, traditional electronic communications have always fallen within this existential space. Telephonic

conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the physicality of the virtual world, outpaced only by the exponential growth in the number of users.

In 2009, for example, approximately 78 percent of the United States actively used the medium as compared to 10 percent in 1995. In the UK, the growth was even more evident with users of the medium rising from 1.9 percent in 1995 to 83.2 percent in 2009.5Noothermethod of communication converges audio, video, and data entities so effectively. Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone. As such, the existential nature of the medium does not negate the reality of its consequences.

Individual users have married, planned their lives, and stalked our children there. Unfortunately, this virtual world is often perceived as a painless alternative to worldly problems, where individuals shed their worries and become perfect in their profiles.

Privacy advocates have often overlooked the negative repercussions of this global medium, arguing zealously that the potentiality of emerging technology precludes governmental interests in monitoring citizens. They argue that the original thrust of the frontier police, directed at ne'er-do-wells intent on compromising the privacy of American citizens, has been refocused on the very individuals that they originally protected. In fact, the two created the electronic- Frontier Foundation(EFF)offeringto"fund,conduct and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional."7 While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through sub urbanization. Beginning with the Industrial Revolution, American society has long been characterized by its distrust of strangers. As media attention increasingly focused on elevated levels of predatory crime perpetrated by non-acquaintances during the 1980s, this fear resulted in a myriad of proactive attempts by both government and citizens to reduce their perceived vulnerability.

Among these were admonitions to children to avoid strangers and lock their doors. While such precautionary measures may have been well served in regards to physical crime, the

advent of technology has lowered traditional barriers and served as an informal invitation for unknown visitors. Many—such as the victims of theft, stolen privacy, and the like—have recognized only too late the dangers of their inattentiveness, while others, yet to suffer negative consequences, remain blissfully unaware of their own vulnerability. In fact, most individuals, young and old alike, are seduced by the soft hum of a device that appears to be the gateway to worlds that were previously restricted. Unfortunately, this fascination may be exploited by those we try most to avoid—criminals and predators. As stated previously, technological advancements have historically led to criminal innovations.

Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the concentration of the urban population, the information or digital revolution has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyber protection even as they add additional door locks and alarm systems to insulate themselves from physical attacks. In fact, it may be argued that the Digital or Information Revolution has created a criminogenic environment in which traditional criminals adapt and new criminals emerge.

Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon. For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. Computer crime has been traditionally defined as any criminal act committed via computer. Computer-related crime has been defined as any criminal act in which a computer is involved, even peripherally.

Cybercrime has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, digital crime, a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, digital crime may be characterized as any of the three depending on case characteristics.

While computer crime and computer-related crime will be used interchangeably throughout the text, cybercrime will only be used to describe that criminal activity which has been facilitated via the Internet. Additionally, students should be advised that a variety of definitions exist, and that such variations have resulted in confusion among legislators and investigators alike. Some authors, for example, argue that any crime that involves digital evidence may be characterized as a computer crime.

This is misleading at best and self-serving at worst. Traditional kidnapping cases in which ransom demands are communicated via telephone will always represent a crime against a person and should not be characterized as a "telecrime." While it is desirable to establish an environment where computers are viewed as potential evidence containers in any case, to redefine traditional predatory crime as cybercrime or computer crime is absurd. Extortion is extortion and will remain such regardless of the method employed to communicate the threat. The result of such hyper-definition is to negate some emerging legislation. This is not to suggest that legislators should cease efforts to specifically

criminalize computer-specific criminal activity. Indeed, further legislation should be pursued to enhance prosecutorial toolboxes, not to replace or supplant traditional mechanisms. Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality. For clarification purposes in this text, computer forensic science, computer forensics, and digital forensics may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.

Individuals seeking a crime have always displayed a remarkable ability to adapt to changing technologies, environments, and lifestyles. This adaptability has often placed law enforcement at a disadvantage, struggling to keep up with criminal innovations. Indeed, the law enforcement community has often failed to recognize the criminal potentiality of emerging technologies until it is almost too late. This trend has proven to be true in contemporary society. Fortunately, much computer-related crime involves non specialist users (e.g., child pornographers, narcotics traffickers, and predators).In fact; the earliest computer crimes were characterized as no technological.

Theft of computer components and software piracy were particular favorites. Hacking, DDoS attacks, phishing, Botnets, and other technologically complicated computer crime scame later. Although the advent of technology has vastly changed the modus operandi of

certain criminal elements throughout history, current advances have changed the very physical environment in which crime occurs. As such, the law enforcement community is experiencing unprecedented periods of uncertainty and ineffectiveness. Many of these problems are associated with the comprehension of the nature of the emerging technology, while others involve questions of legality and sovereignty.

Unfortunately, legislative bodies and judicial authorities have been slow to respond to such inquiries, and law enforcement has been forced to develop investigative techniques without adequate legal foundations. At the same time, the lack of technological knowledge, allocated resources, and administrative apathy traditionally associated with the law enforcement community hampers even the most mundane investigation. So, while the investigators of computer-related crime must display levels of ingenuity comparable to sophisticated criminal entrepreneurs, traditional investigators and policymakers are ill-equipped to do so.

4.8 INCIDENT RESPONSE IN CYBER CRIME:

Incident handling is a generalized term that refers to the response by a person or organization to an attack. An organized and careful reaction to an incident can mean the difference between complete recovery and total disaster. This paper will provide a logical approach to handling two common forms of attack - virus outbreak and system compromise. The method that this article will propose includes the following sequence of steps that should be followed in the case of all types of attack

Preparation:

Comprehensively addressing the issue of security includes methods to prevent attack as well as how to respond to a successful one. In order to minimize the potential damage from an attack, some level of preparation is needed. These practices include backup copies of all key data on a regular basis, monitoring and updating software on a regular basis, and creating and implementing a documented security policy. Regularly scheduled backups minimize the potential loss of data should an attack occur. Monitoring vendors' and security web sites and mailing lists is a good way to keep up to date with the state of the software and patches. It is necessary to update software in order to patch vulnerabilities that are discovered. It is also vital to update anti-virus software in order to keep system

protection up-to-date. A documented security policy that outlines the responses to incidents will prove helpful in the event of an attack, as a reliable set of instructions.

Identification of Attack:

While preparation is vital for minimizing the effects of an attack, the first post-attack step in Incident handling is the identification of an incident. Identification of an incident becomes more difficult as the complexity of the attack grows. One needs to identify several characteristics of an attack before it can be properly contained: the fact that an attack is occurring, its effects on local and remote networks and systems and from where it originates.

Containment of Attack:

Once an attack has been identified, steps must be taken to minimize the effects of the attack. Containment allows the user or administrator to protect other systems and networks from the attack and limit damage. The response phase details the methods used to stop the attack or virus outbreak. Once the attack has been contained, the final phases are recovery and analysis.

Recovery and Analysis:

The recovery phase allows users to assess what damage has been incurred, what information has been lost and what the post-attack status of the system is. Once the user can be assured that the attack has been contained, it is helpful to conduct an analysis of the attack. Why did it happen? Was it handled promptly and properly? Could it have been handled better? The analysis phase allows the users and administrators to determine the reason the attack succeeded and the best course of action to protect against future attacks.

Incident Handling - Viruses

• Preparation

Viruses can cause irreparable harm to important files and records. The home and small office user is at even higher risk than larger organizations because the user often works with one computer or stores important information in a single location. Unlike larger

organizations that have data spread across many systems in several locations, a virus outbreak in a home or small office could permanently destroy important data. This puts greater emphasis on the need for creating backups of all information. Additionally, backup disks should be kept in a separate location, away from the computer. This ensures that in case of an incident such as fire or theft of hardware that a backup copy of all information is still available. The second crucial step in preparing for an attack is to install anti-virus software. Anti-virus software is readily available, easy to install and operate and is affordable. New viruses are created frequently, so it is important to be diligent with anti-virus software maintenance. Almost all anti-virus vendors make updates available on their websites. Users should update their anti-virus software on a regular basis.

• Identification of Virus Attack

Viruses are particularly potent and frightening because of their ability to spread quickly to 'friendly' computers. Just think of the public relations nightmare your company could endure if you're the address book in your e-mail program was used to spread a virus to all your suppliers' and your customers' computers. Early identification of an incident is crucial to ensuring that the virus does not spread to other computers. It is crucial that users are familiar with the symptoms of a virus attack, such as mass e-mailing, file destruction or other malevolent actions the results of which can be seen immediately. Stealthy viruses require a bit more attention. The user should be aware that periodic anomalous behavior on a system is not always an indicator of a virus attack. Other factors may cause the erratic behaviour; however, for the sake of security, the user should scan the computer comprehensively to clearly identify the cause. Configuring the anti-virus software to do real-time scanning of files and to periodically do complete system scans helps to both prevent and identify viruses.

• Containment:

Containment of the virus is pivotal in limiting the effects. Many viruses spread themselves automatically. If a non-replicating virus infects a single computer, containing the virus is fairly straightforward. The administrator, or user, should disconnect network access including shared directories and other components that may allow the virus to infect files and programs on other machines. Anti-virus software often has a "rescue" component that allows an administrator to scan and clean a system by booting from a specialized floppy disk or CDROM. If available, these tools should be utilized to disinfect the system. Should the anti-virus software fail to clean the system or lack the features necessary to do the cleansing, it is advisable to try other software packages that may provide more

comprehensive coverage. If the system has been altered beyond repair, the last resort is to clear the system entirely and reinstall the operating system and software. If reinstalling, care should be taken to use software that is known to be uninfected and to completely reformat the hard drive to assure the eradication of the virus.

• Recovery and Analysis: Viruses cause varying degrees of destruction- some exist merely to replicate; others attach to and destroy files and programs. Anti-virus programs can generally restore files to their original state, but there are exceptions. If there is doubt to the reliability of the data held within a file, the user should compare the damaged file to a backup copy in order to assess whether or not damage has been sustained. Once the system or systems have been returned to full operation, analysis should be done to determine where the defenses failed. Does fault lie in the anti-virus software, or the frequency and reliability of updates? Or did some user behaviour - such as opening files from an unknown or untrusted source - allow the system to become infected? Once the attack was identified, were appropriate and sufficient steps taken to minimize the damage that the system sustained? Analysis of the incident allows the user to learn from the unfortunate incident and ensure that it does not happen again.

System Compromise

• Preparation

System compromise is an attack in which an intruder breaks into a computer and, either sitting directly in front of it or from a remote network, is able to use that computer. The attacker typically has total access to a system and all information contained therein including files, applications and potentially any other system connected to it. Managing system compromise is more daunting than managing virus outbreaks. The basic steps to help prepare in case of system compromise are basically the same as are used in preparation for virus outbreaks. All vital information should be backed up on a regular basis. Software updates are also crucial. System compromise often arises due to security vulnerabilities in common software, particularly in operating system software.

Users and administrators should be sure to maintain current software patches in order to protect against attacks. Patches are available through vendors' websites. Users can learn

about the latest patches by monitoring vendors' web sites, mailing lists and user forums related to the software and to security. In order to prevent against unauthorized intrusion into a system, users should implement firewalls. Just as anti-virus software is the cornerstone of a virus prevention strategy, firewalls are extremely important in preventing unauthorized individuals from accessing network services and resources. Like anti-virus software, firewalls are relatively affordable and easy to use - they not only protect against intrusion, but some can be configured to notify the user if an intrusion is being attempted.

• Identification

Systems compromise attacks are often indicated by missing or modified files, changes to the system configuration and services, greater memory and disk usage and unidentified network connections. Attackers will often seek to hide any indication of the intrusion by replacing files and programs with versions that protect the attacker. Programs that act normally on one occasion and strangely the next, as well as files and programs that have their time, date or size information modified may be indicative of an unauthorized intrusion. Comparison against backup copies may reveal changes to files. Users and systems administrators can identify potential systems compromise attacks by monitoring network traffic and processes. The new wave of Intrusion Detection Systems (IDS) is extremely helpful in allowing for the monitoring of systems. By actively monitoring the network for known signs of attack and other anomalous conditions, an IDS notifies users as soon as it detects the event. IDS are useful in complex networked environments and where minimal technical staffing is available. By automatically monitoring and notifying users, an IDS can offload some responsibility from an overburdened administrator, making them invaluable resources for users and administrators in small offices and home offices.

• Containment

Containment of an intrusion involves some effort on the part of the administrator. First, the administrator should freeze the current system as soon as an intrusion is suspected. This includes disconnecting the system from the network, stopping the operating system and disallowing anyone to use the system. As an operating system runs and people use the system files are naturally modified and updated depending on what they are doing. This normal functionality often erases important information that can be used to detect and trace an intrusion; therefore it is very important to stop the system as soon as possible after an attack is discovered. If possible, it is advisable to duplicate the hard disk of the system. This allows the administrator to begin the cleanup process on one disk and to give the other to an expert to determine the exact source and cause of the intrusion.

• Recovery and Analysis

The most devastating but least-effort method of cleaning up a compromised system is to wipe the hard disk clean and re-install the operating system and software allowing a faster return to normal operation. A more painstaking approach is to compare each individual file and program against a copy known to be original in order to determine if any modifications have been made. It is important to do a minimal level of analysis in order to determine the cause of the intrusion. Once a cause is determined, changes to the environment should be made to avoid future attacks by that method. This includes updating affected software, access control methods that allow only certain users, systems and networks to use the services, firewalls and intrusion detection systems.

A combination of these changes can provide a safer and more secure working environment. Analysis of the attack provides several benefits. The user and administrator can determine the shortcomings in existing security policies, installation methods and configurations that allow attacks to succeed. Users and administrators should periodically review existing installations, configurations and security policies. New attacks and security vulnerabilities are found often and updating the existing environment can minimize the threats of future attack.

4.9 Digital Forensics:

Digital forensics is a key component in Cyber Security. Many people hear the term forensics, or computer forensics, or digital forensics and instantly think, that's just for law enforcement, but the truth is, digital forensics has a key place on every cyber security team. In fact, without it, chances are your organizations Security posture and maturity will fail to see its full potential. Digital forensic practices stem from forensic science, the science of collecting and examining evidence or materials. Digital or computer forensics focuses on the digital domain including computer forensics, network forensics, and mobile forensics. In the event of a cyber-attack or incident, it is critical investigations be carried out in a manner that is forensically sound to preserve evidence in the event of a breach of the law. Far too many cyber-attacks are occurring across the globe where laws are clearly broken and due to improper or non-existent forensic investigations, the cyber criminals go either unidentified, undetected, or are simply not prosecuted.

Malware Forensics

Malware is a type of software intentionally designed with malicious functionalities. The goal of malware forensics is to find out:

• What the malware can do (and what it does in a particular situation)

• To which family it belongs to (ransomware, keyloggers, and remote administration tools)

• How it can be detected and blocked, and

• How it can be cleanly removed from an infected system

To achieve these goals, there are two approaches: static analysis and dynamic analysis. Each approach has its own pitfalls and advantages. Static analysis examines the binary without running it. It is the only option when the malware cannot be run, i.e. taken from a partial memory dump, missing pieces, or having an unavailable architecture. It tells the analyst everything the program can do, but this approach is less precise because of the need to reason about the program behavior without actually executing the code. By contrast, it achieves a larger coverage: one can reason about all possible executions at the same time. Dynamic analysis runs the program and observes its behaviour. It tells the analyst exactly what the program does when it is executed in a given environment and with a particular input. It is more precise because it can observe the instructions executed and the values of registers and memory; however, it achieves a smaller coverage because it observes one execution path at the time.

A general approach to malware analysis would be:

1. Set up a controlled, isolated laboratory in which to examine the malware sample

2. Perform behavioral analysis to examine the sample's interactions with its environment

3. Perform static code analysis to further understand the sample's inner workings

4. Perform dynamic code analysis to understand the more difficult aspects of the code

5. If necessary, unpack the sample

6. Repeat steps 2, 3, and 4 (order may vary) until analysis objectives are met

7. Document findings and clean up the laboratory for future analysis

The following section describes each step with the common and popular tools used to achieve the goal. Examining malicious software involves infecting a system with the malware sample and then using the appropriate behaviour analysis tools to observe its interaction with the system. This requires an isolated laboratory environment that you can infect without affecting your production environment. The most common and flexible way is to use virtualization software (e.g., VMware or VirtualBox). To understand the threat associated with the sample, the analyst needs to examine its behaviour in the controlled environment already setup in the previous step. He uses Process Monitor to study the process, network, file, and registry interactions between the malware and the operating system.

Process Monitor is a common tool for capturing the following events:

Registry: Capture registry keys query, read, and creation operations.

File system: File creation, writing, deletion from local hard drives and network drives.

Network: Show the source and destination of TCP/UDP traffic, but it doesn't show the data.

Analysts use Wireshark to capture data. Packets can be filtered based on source destination IP/port by Process Monitor.

Process: Shows processes and threads creation and exit, etc.

Profiling: Checks the amount of CPU time used by each process or the malware being studied and the memory use

To check if the sample is a known binary based on its hash or if it is similar to something already known based on its signature, the analyst could submit it to Virus Total. Virus Total

is a sandbox tool for malware identification owned by Google. The tool has the biggest repository of malware and known file types around. Malicious binaries are typically stripped of all symbols, obfuscated and packed. In addition, they implement plenty of anti-debugging and anti-analysis tricks and checks for analysis environments. Packing a program is compressing or encrypting the instructions and data in order to save disk space.

It's widely used by malware writers. Many packers automatically include anti-disassembly, anti-debugging, and anti-VM techniques to further complicate the analysis. The packer can be identified based on its signature or by using heuristics. PEiD is a popular tool that can identify most common packers, cryptors, and compilers for PE files. It packs more than 600 different signatures in PE files, which make its detection rate higher than that of other similar tools. There are several heuristic techniques to determine whether a program is packed, including sections with high entropy, weird section names, and few entries in the import table, etc. Mandiant's Red Curtain tool computes entropy of sections. High entropy means that the program is likely packed or encrypted. The tool also scans for packing signatures and computes a threat score.

There are several approaches to unpacking a program. One first approach could be to manually reverse-engineer the packing stub and write the corresponding unpacking tool, but this is complex and time-consuming. An automatic and dynamic approach could be dumping the binary containing the unpacked program. In a few cases, the program can be unpacked automatically using a tool (e.g., the UPX tool, using –d option). PEiD comes with a set of plugins, including an UPX unpacker.

Disassemblers are among the tools that can be used to statically analyze binary programs and further understand the malware's inner workings. These tools do not require the analyzed module to operate; it can be safer to use static analysis if it is known that the module under analysis is malicious. A disassembler converts machine language into assembly language. IDAPro is popular tool for doing this job. In order to determine the higher-level logic of a function, such as loops, switches, and conditions, the malware analyst can use a decompiler. A decompiler converts assembly code into source code in a higher-level language such as C++ or C. Paid versions of IDAPro come with a C/C++ decompiler called Hex-Rays Decompiler. An alternative is to use a similar tool called Snowman.

• Memory Forensics

Memory forensics is the process of investigating a memory dump to locate malicious behaviors. The dump is a snapshot capture of RAM memory at a specific point of time; it can be a full physical memory dump, a crash dump, or a hibernation file. The investigator extracts useful artifacts from memory, including running processes, URLs, passwords, encryption keys, kernel modules, shared libraries, open sockets, active connections, and open registry keys. That information can be accessed by obtaining and analyzing the target computer's physical memory dump.

A general approach to memory forensics would acquire and analyze physical memory. Memory dump acquisition: can be performed using a program installed on the system, such as win32dd, win64dd, dumpit, or dd or by using dedicated hardware such as an internal acquisition card (PCI card), or sniffing direct memory access (DMA) transfer, or using a FireWire port. The difference is that the software may alter the system, in contrast to the use of hardware. However, using hardware may crash the system or lose information, in the case of FireWire. In addition, the hardware must be installed on the machine before an incident occurs. Memory dump analysis: Many tools offer digital artifacts and analysis facilities. Volatility is the most popular memory forensics framework. It can extract digital artifacts from multiple types of memory (crash dump, core dump, hibernation file, etc). It provides an in-depth visibility into the runtime state of the system.

Rekall is an advanced memory analysis solution. It is basically a fork of the Volatility memory analysis framework maintained by Google's incidence response team. To start the analysis, summary information of the dump can be viewed. This information includes the operating system version and target architecture (32 or 64 bits). The most commonly used analysis approach then is to list the processes that were running in the system, the loaded kernel modules, and shared libraries to locate malicious modules. The analysis can also cover other data, such as registry keys. In addition to the active processes, the analyst should keep track of terminated and hidden processes, since they might also load malicious modules. The analysis may end when malicious files are dumped. Then malicious file analysis comes to play as described in the previous section. document the findings and analysis results in a report that summarizes the answers to the predefined questions. The analysis report covers, but not limited to, screenshots, notes, and observations.

• **Email Forensics**

Emails are the main channel for worms, phishing, and the transportation of spam. Email forensics involves investigating email content and sources to reveal key information, such as the recipient's identity, the trace path traversed by the message, the application used to compose the email, the timestamp when a message was generated, a unique message ID, etc.

Typically, email forensics consists of the following steps:

• Examining sender's e-mail address

• Examining message initiation protocol (HTTP, SMTP)

• Examining message ID

• Examining sender's IP address.

This involves investigation of port scanning metadata and keyword searching. There are several approaches to email forensics such as header analysis, server investigation, client-side mailer fingerprint, network devices investigation, and bait tactics. Many tools may assist in the study of source and content of e-mail message so that an attack or the malicious intent of the intrusions may be investigated. The following is a non-exhaustive list of email forensics tools

• MailXaminer

• Add4Mail

• eMailTrackerPro

• AccessData's FTK

• Paraben E-Mail Examiner

Smartphone Forensics:

Smartphone devices contain sensitive personal information such as contact lists, SMSs, calls, pictures, etc. This information can be used by attackers to impersonate the owner's identity, so it is risky if it is lost or stolen. That's why smartphones become an inevitable source for digital forensics. There are three primary approaches to smartphone forensics which focus on extraction of data that might be rightly challenged in a court of law.

Manual Acquisition: The investigator browses the smartphone and takes pictures of each screen that contains important information. This technique does not alter the device and no tools are required to perform data acquisition. However, only data visible to the investigator can be recovered since only the user interface is used. Physical Acquisition: The investigator clones the smartphone storage device and then normal disk forensic techniques are used (see Disk Forensics section). Logical Acquisition: In this technique, little manual intervention or cloning is required. Here data available on the smartphone is acquired by automated tools for synchronizing the device and PC. With this technique, the investigator can't acquire deleted data and unallocated spaces.

The following is a list of the popular tools available for smartphone forensics:

- Andriller
- XRY
- Oxygen Forensic
- Ufed Touch
- Droidspotter
- Mobiledit Forensic

Disk Forensics

The goal of disk forensics is to acquire a copy of data resident on hard drives and USB memory sticks, analyzing it to extract digital evidence. The acquisition can be performed at the file level or the sector level. At the file level, the investigator can't acquire deleted files and unallocated spaces. At the sector level, however, the investigator can acquire an exact copy of the device storage. If the storage is corrupt or damaged, then the investigator

relies on file carving, which may recover data if the files' metadata are lost. The most popular tools are the Sleuth Kit, Digital Forensic Framework, FTK, and EnCase.

Cloud Forensics

Cloud forensics involves inspecting cloud components, which include logs, virtual machine disk images, volatile memory dumps, console logs, and network captures. Cloud forensic tools collect data from the cloud, image the instances, and recover data from cloud instances. FROST is a forensics tool for OpenStack.

Log Forensics

Logs generated by the operating systems and applications are segregated and parsed to generate useful information. Correlation mechanisms are applied to find relationships between logs and external or internal events.

4.10 Network Security:

Network security is an integration of multiple layers of defenses in the network and at the network. Policies and controls are implemented by each network security layer. Access to networks is gained by authorized users, whereas, malicious actors are indeed blocked from executing threats and exploits. Our world has presently been transformed by digitization, resulting in changes in almost all our daily activities. It is essential for all organizations to protect their networks if they aim at delivering the services demanded by employees and customers. This eventually protects the reputation of your organization. With hackers increasing and becoming smarter day by day, the need to utilize network security tool becomes more and more impotent.

Types of Network Security

1) Antivirus and Antimalware Software

2) Application Security

3) Behavioral Analytics

4) Data Loss Prevention (DLP)

5) Email Security

6) Firewalls

7) Intrusion Prevention System (IPS)

8) Mobile Device Security

9) Network Segmentation

10) Security Information and Event Management (SIEM)

11) Virtual Private Network (VPN)

12) Web Security

13) Wireless Security

14) Endpoint Security

15) Network Access Control (NAC)

1) Antivirus and Antimalware Software: This software is used for protecting against malware, which includes spyware, ransomware, Trojans, worms, and viruses. Malware can also become very dangerous as it can infect a network and then remain calm for days or even weeks. This software handles this threat by scanning for malware entry and regularly tracks files afterward in order to detect anomalies, remove malware, and fix damage.

2) Application Security: It is important to have an application security since no app is created perfectly. It is possible for any application to comprise of vulnerabilities, or holes, that are used by attackers to enter your network. Application security thus encompasses the software, hardware, and processes you select for closing those holes.

3) Behavioral Analytics: In order to detect abnormal network behaviour, you will have to know what normal behavior looks like. Behavioral analytics tools are capable of automatically discerning activities that deviate from the norm. Your security team will thus be able to efficiently detect indicators of compromise that pose a potential problem and rapidly remediate threats.

4) Data Loss Prevention (DLP): Organizations should guarantee that their staff does not send sensitive information outside the network. They should thus use DLP technologies, network security measures, that prevent people from uploading, forwarding, or even printing vital information in an unsafe manner.

5) Email Security: Email gateways are considered to be the number one threat vector for a security breach. Attackers use social engineering tactics and personal information in order to build refined phishing campaigns to deceive recipients and then send them to sites serving up malware. An email security application is capable of blocking incoming attacks and controlling outbound messages in order to prevent the loss of sensitive data.

6) Firewalls: Firewalls place a barrier between your trusted internal network and untrusted outside networks, like the Internet. A set of defined rules are employed to block or allow traffic. A firewall can be software, hardware, or both. The free firewall efficiently manages traffic on your PC, monitors in/out connections, and secures all connections when you are online.

7) Intrusion Prevention System (IPS): An IPS is a network security capable of scanning network traffic in order to actively block attacks. The IPS Setting interface permits the administrator to configure the ruleset updates for Snort. It is possible to schedule the ruleset updates allowing them to automatically run at particular intervals and these updates can be run manually on demand.

8) Mobile Device Security: Mobile devices and apps are increasingly being targeted by cybercriminals. 90% of IT organizations could very soon support corporate applications on personal mobile devices. There is indeed the necessity for you to control which devices can access your network. It is also necessary to configure their connections in order to keep network traffic private.

9) Network Segmentation: Software-defined segmentation places network traffic into varied classifications and makes enforcing security policies a lot easier. The classifications are ideally based on endpoint identity, not just IP addresses. Rights can be accessed based on location, role, and more so that the right people get the correct level of access and suspicious devices are thus contained and remediated.

10) Security Information and Event Management (SIEM): SIEM products bring together all the information needed by your security staff in order to identify and respond to threats.

These products are available in different forms, including virtual and physical appliances and server software.

11) Virtual Private Network (VPN): A VPN is another type of network security capable of encrypting the connection from an endpoint to a network, mostly over the Internet. A remote-access VPN typically uses IPsec or Secure Sockets Layer in order to authenticate the communication between network and device.

12) Web Security: A perfect web security solution will help in controlling your staff's web use, denying access to malicious websites, and blocking

13) Wireless Security: The mobile office movement is presently gaining momentum along with wireless networks and access points. However, wireless networks are not as secure as wired ones and this makes way for hackers to enter. It is thus essential for the wireless security to be strong. It should be noted that without stringent security measures installing a wireless LAN could be like placing Ethernet ports everywhere. Products specifically designed for protecting a wireless network will have to be used in order to prevent an exploit from taking place.

14) Endpoint Security: Endpoint Security, also known Network Protection or Network Security, is a methodology used for protecting corporate networks when accessed through remote devices such as laptops or several other wireless devices and mobile devices. For instance, Comodo Advanced Endpoint Protection software presents seven layers of defense that include viruscope, file reputation, auto-sandbox, host intrusion prevention, web URL filtering, firewall, and antivirus software. All this is offered under a single offering in order to protect them from both unknown and known threats.

15) Network Access Control (NAC): This network security process helps you to control who can access your network. It is essential to recognize each device and user in order to keep out potential attackers. This indeed will help you to enforce your security policies. Noncompliant endpoint devices can be given only limited access or just blocked.

• **Technical Network Protection**: Technical Network Protection is used to protect data within the network. Technical network protection guards both stored and intransit data from malicious software and from unauthorized persons.

• **Physical Network Protection:** Physical Network Protection, or Physical Network Security, is a network security measure designed to prevent unauthorized people from physically

interfering with network components. Door locks and ID passes are essential components of physical network protection.

• **Administrative Network Protection**: Administrative Network Protection is a security method that control a user's network behaviour and access. It also provides a standard operating procedure for IT officers when executing changes in the IT infrastructure. Company policies and procedures are forms of Administrative network protection

Realms of Cyber World: The need for information security has ceased to be a subject of debate in technology circles. The expectations, the context and the need probably differ, however one sees a consensus on the need to secure and protect information. In the technology landscape, where jargon and acronyms occur as frequently as the tides that wash ashore, the term cyber security has grabbed a lot of attention. International Telecommunication Union (ITU) refers to cyber security as –'Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.' Professionals, enterprises and even nations seem to focus on cyber security today.

While the people at large may not ponder much, for IT professionals it may raise a few questions. Some of them are likely to be -are the terms information security and cyber security synonyms, if not what's the difference? Is cyber security is a sub set of information security or are the two entirely different? Multiple definitions that allude to the different views on cyber security are likely to be available. However it is important that we understand the core behind cyber security than get hindered by the definitions. The focus on threats, risks and controls relevant to the cyber world is the realm of cyber security. This does not mean that security in the cyber world was not addressed in the information security legacy that we inherited and that has developed over the years. The footprint of the 'cyber' aspect though, was rather limited. This limited focus was not deliberate but merely reflected the reality of the day where connectivity to cyber space was less extensive and controlled. Hence the risks posed by the cyber world were not as extensive as they are today. Changes in the environment triggered a focus on cyber security. The changes have been varied and extensive. The changes have not been unidimensional but have encompassed a wide landscape. The traditional view about architecture, technology, its delivery and utilization have all changed. The holy grail of technology available to a few qualified professionals is now available to the world at large. Within a short span of time, innovative and unthinkable concepts like Bring Your Own Device (BYOD) and Mobility,

Cloud Computing, Social Networks, Internet of Things (IoT) have become reality of the day.

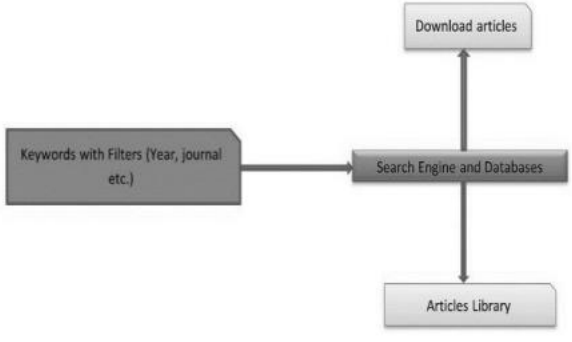
This imperative has been embraced for sure–in some instances with open arms and in few other cases grudgingly. The underlying enabler for the change is connectivity that has been provided by the cyber world. The innovative and diverse leveraging of the cyber world has increased the number of cyber citizens and also the traffic flows. The perimeter has traditionally been the frontier that separated the trusted internal network from the un-trusted external network. The gatekeepers in the form of layer 3-4 firewalls provided the much needed assurance and resilience to protect from external threats. In some instances it was complemented by Intrusion Detection/Prevention Systems. The 'internal' elements with patched end points and antivirus software fortified the network. Alas this simplistic model, though essential Even today no longer provides the level of assurance it provided earlier.

The BYOD program saw an influx of personal devices with a variety of operating systems. The enterprise no longer owned and controlled all the end points. The devices that traditionally were outside the trusted perimeter were now connected to the internal network. These devices tip toed inside the perimeter due to their physical proximity; however some devices even when physically remote became part of the trusted network. Virtualized servers hosted by IaaS and PaaS providers and applications provided by SaaS that are physically away from the perimeter need to be part of the trusted network. The traditional firewalls that had no visibility on the application layer were not much useful in regulating traffic to the cloud since IP addresses changed at irregular intervals.

CHAPTER 5

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

With the rapid progress of internet technology and systems, the opposite is also true that cybercrimes and assaults are increasing at an alarming rate. To counter and defeat these cybercriminals and their smart techniques, we need AI-based techniques in our cybersecurity systems to enhance the cyberspace security more effectively.



Techniques of AI	Applications in cybersecurity
Neural nets	1.For intrusion detection and prevention system 2.Very high-speed of operation 3.For Denial-of-service (DoS) detection 4.For forensic investigation 5.Warm detection 6.Fuzzy logic
Intelligent agents	1. Proactive and reactive 2. Agent communication language 3. Defense against Distributed Denial-of-service (DDoS)
Expert systems	1. For network intrusion detection 2. For decision support 3. Knowledge base 4. Inference engine

AI provides several advantageous to deal with cybersecurity issues, some of the benefits AI provide are as follows:

Unlike traditional technology which focused mainly on the past and totally depended on known cyberattacks. If there is new cyber-attack happens the conventional systems are unable to detect the changes and thus leaving a blind spot during unusual attacks. AI can detect new and complex variations in attack flexibility. In the future, AI systems will be more sensitive to detect similar changes. The learning and adaptation capacity of AI machines is superior and can detect faster, anomalous, and more accurate operations. This ability of AI systems is more important when cyber-attacks are becoming more refined and cybercriminals are coming up with new and inventive methods.

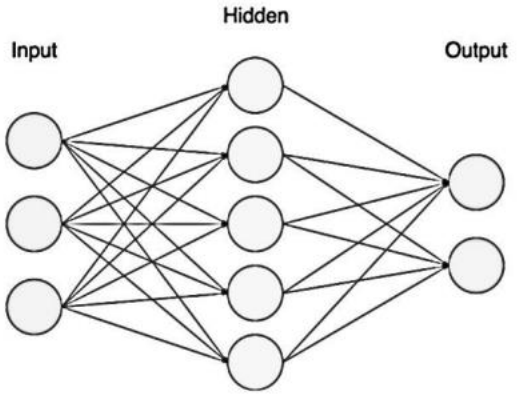
AI has the ability to deal with large amounts of security data. Because AI includes self-contained security systems that can detect and respond to attacks. The amount of data breaches received daily is unbearable for security personnel; however, automatically detecting and responding to threats has helped to reduce experts' workload. Moreover, AI can better manage these cyberattacks than any other method. When a significant amount of security data is generated and transferred over the network daily, network security

analysts will find it increasingly difficult to detect and monitor attack elements accurately and quickly. This is where AI can help by increasing the frequency with which suspicious type of behavior is mentioned and detected. This can assist network security officers in reacting to situations they haven't seen before, obviating the need for time-consuming people analysis.

Application behavior and regular network traffic are studied by AI security systems over time. In this way detecting the threats over time, AI make a baseline of what are the normal patterns. If any change or deviation found in the normal pattern, AI security system will detect the attacks.

Neural networks, expert systems, machine learning, deep learning, and data mining are just a few of the AI security models that can be used to effectively deal with cyberattacks and threats. AI-based methods can be used to make intelligent decisions in the cyberspace. In this paper we have highlighted all these AI techniques and described briefly in the following sections.

Artificial Neural Networks (ANNs) was created by Frank Rosenblatt in 1957 as statistical learning technique that function like neurons in human brain. ANN technique mimicking neurons in terms of a mathematical equation where the model read enormous samples to produce a target value. ANNs are highly capable to understand, learn and solve the problems in different areas. It's also capable to solve noisy and incomplete data samples. In the cyber defense framework, ANNs have been used in the early warning phase, prevention phase, detection phase, and response phase. ANNs are very useful in intrusion detection systems (IDS) because of the adaptability. When used in cybersecurity, ANNs could be used to study traffic flow in security networks, allowing them to detect intrusions before they occur and then stop cyber-attacks through perimeter defense. ANNs have the potential to learn from past network activities to stop later threats. A typical illustration of ANN is shown in Fig



The Cascade Correlation Neural Network (CCNN) was used in a study of cybersecurity, which stepwise adds new hidden units to the hidden layer. When new events are detected, this system adds new hidden nodes to the network, training those nodes with the newly collected data. In this way CCNN provide runtime adaptive and scalable system. To learn from desktop-platform traffic patterns to detect port scanning to mobile networks, the CCNN only trains the network with new data, ignoring the entire network with the original data. The identification and evaluation of ANN port-scanning is analogous to other methods such as Decision trees, according to this investigation. ANNs, in contrast to manual methods, have the ability to detect patterns in highly nonlinear problems with a high rate of classification. Using previously transferred data over the network, ANNs can automatically place normal and abnormal network patterns. ANNS is used to scan network traffic by network security tools such as firewalls, network hubs, and intrusion detection systems. A more advanced form of ANN is Deep Neural Network (DNN), with high advantage it not only protects the security system from cyber-attacks, but also predicts that such attacks will occur in the future. A study was carried out to detect cyber-attacks using DNN methods of AI-based security program, the results showed 85% success rate. This achievement of DNN opened a new chapter of cybersecurity known as cyberattack prediction.

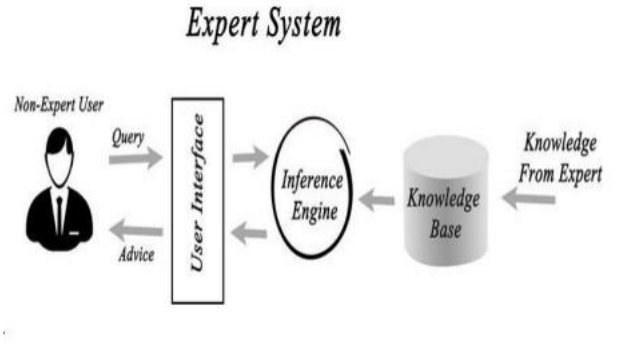
In AI, an expert system is a computer software application that assists a human expert in deciding. The system consists of two parts; knowledge base and inference engine, both collectively forms security rules. Cybersecurity expert system decisions are based on security guidelines. Expert systems modeling has applications in medical diagnosis, finance, and cyberspace. Expert systems are diverse, from small to large and complex hybrid systems which dealing with sophisticated issues and problems. The cybersecurity expert framework consists of a knowledge base phase which describe the knowledge of the domain as well

as operational knowledge of the rules of security decisions, and the inference engine phase which is involved to get responses from the knowledge base and deduce new facts.

Expert systems can be employed in different problems based on how the reasoning could be done. In one approach referred to as, "case-based reasoning (CBR) approach", a particular problem is solved by recollecting previous similar cases, then a solution is determined by adapting the past solution to a new problem case. In this way new solutions are analyzed to improve the accuracy and learning capacity of the system. Rule-based systems (RBS) is another approach to solve problems, characterized by rules to solve problems defined by experts. The rule-based system consists of two sub-systems: condition part and the action. Condition part evaluation used to analyze the problems, then the action to be taken is determined.

Cybersecurity expert system fighting against cyber-attacks using some guidelines and rules. For instance, it evaluates the process against the knowledge base, if the process is good and known, then the security system considers it safe, if not the system declares it as a threat and then terminate the process. If the knowledge base lacks such a process, the system finds the sets of rules in the inference engine to determine the machine's state. The machine can be in one of three states: severe, moderate, or safe. The system notifies the manager or user of the machine's status based on the state of the machine, and then the inference as detected by the knowledge base.

A rule-based cybersecurity expert system model may thus have the decision-making capacity of a security expert in an intelligent cybersecurity framework built to solve complex cybersecurity issues, as well as by information reasoning. As a result, cybersecurity expert system modelling, based on its computing capabilities and ability to make intelligent decisions, can be a valuable component in AI-based cybersecurity.



Intelligent agents (IAs) are self-controlled systems with internal decision-making mechanism and a personal objective. It evaluates threats through sensors and monitor the domain via actuators. It controls the actions until a particular objective is achieved. These systems have proactive and responsive characteristics, and when communicating with other autonomous agents, can understand and respond to changes in their domain. In this way, these intelligent agents are adaptive in the sense these can learn and communicate with their environment. IAs are proved effective to stop Distributed Denial of Service (DDoS) attacks. How these agents can be used against distributed cyber-attacks? The answer is by constructing artificial "Digital police" which must include mobile intelligent agents, which obviously required to deploy infrastructure to provide firm support to the mobility and communication of cyber agents.

Search is a critical thinking approach which can be employed in different situations especially when there is no alternate approach for critical thinking. We also using search strategy on daily basis as a subconscious problem solving method. A prior knowledge about search strategy is required before performing search algorithm. These search algorithms have been embedded or added into almost every intelligent program and positively affecting the whole intelligent system. There are variety of methods of search security system in AI such as the αβ-search estimation which is employed as a part of various projects. The search estimation was created for computer chess. It employs the critical thinking strategy of "isolate and vanquish," which is particularly useful in primitive leadership when two foes are deciding on their most ideal activities.

Bio-inspired computing in AI is a newly emerged field consisting of smart algorithms and techniques that uses bio-inspired behaviors and attributes to tackle variety of academic and environmental sophisticated problems. Examples of bio-inspired computing techniques are

Evolution Strategies (ES), Ant Colony Optimization (ACO), Artificial Immune System (AIS), Particle Swamp Optimization (PSO) and Genetic Algorithms (GA), these techniques are commonly employed in the cyberspace. This technique is also used in the classification of computer malwares. In the classification of computer malwares these techniques primarily used to optimize features and parameters for the classifiers. For example, PSO and GA techniques were employed to the improve the efficiency of malware detection system. In another study fuzzy logic and GA were used for detection of intrusion. The GA was used to create a digital signature of a network segment using glow analysis to predict network traffic behaviour for a specific time. In addition, the fuzzy logic method was used to determine whether or not an instance on the network was anomalous. The evaluation was conducted using network traffic from a university, and the results were 96.53 percent accuracy and 0.56 percent false notification.

Machine learning is a branch of AI that deals with teaching machines to learn new things and make decisions based on data using algorithms. Mathematical techniques that allow for the extraction of data, the discovery of patterns, and the drawing of conclusions from it are all closely related to machine learning. Classification and regression are the two most important methods of ML technology.

1. Supervised learning,

2. Unsupervised learning,

3. Semi-supervised learning,

4. Reinforcement Learning are all types of the ML technology

Another learning known as deep learning is a knowledge about machine learning that uses data to train computers how to do things that previously only humans could do. This is accomplished by simulating the human brain's data interpretation mechanism. Deep learning is based on the principle that as we build larger neural networks and train them with more data, their performance improves.

ML and DL have been shown very important in resolving cybersecurity issues. ML methods have wider applications in the security system. Examples include spam filtering, network anomalies analysis, botnet tracking, and tracking user behavior anomalies. Similarly, DL has been proved effective in the detection of malware and network intrusions.

Those institutions implemented AI techniques in the cybersecurity operations have been benefited significantly. For example, the ROI of some institutes have been increased by adopting AI in the cybersecurity issues. Siemens AG created AI based Siemens Cyber Defense Center (CDC) which is characterized by its high speed, self-controlled and adaptive. He used this system in Amazon Web Services (AWS). Due to AI application the system was estimated 60000 attacks per unit time. The overall capability was managed easily with less than 12 members as well good maintenance of system performance. AI in cybersecurity can identity new threats by analyzing previous threat patterns. This approach of AI is useful to same time and energy used in the investigation and identification of threats and attacks. It has been revealed AI is very useful in the identification and reactions to threats with low cost (average of 12% cost reduction).

Today, AI can provide enormous solutions to cybersecurity problems as the cybersecurity system is transforming from traditional and manual approaches towards automated algorithm mitigation. Unlike traditional technology which relies mostly on already identified intruders and intrusions and thus leaving a blind spot during unusual intrusion activities, AI can detect new, and complex change in the attack extensibility. These drawbacks of conventional security technology have now been resolved by AI technology. For example, privileged internet activities can now be monitored and any change in privileged access operations can be regarded as a potential threat. AI predictive methods offer an edge to security teams which is important to stop attacks before causing any destruction. Dark trace (United Kingdom company) used ML technology for the detection of patterns and threats in many areas such as retails, manufacturing, energy, and transportation firms. Large amount of data and improvement of network security systems can be managed through AI-based techniques. The huge volume of active security issues is overwhelming for the security experts. Autonomous detection and response to attacks by AI has decreased the load of security groups. When security data in massive amount produced and transferred on daily basis, then it's a challenging task for the security experts to manage it. Hence, AI can help to scale-up the analysis of doubtful processes and activities. Furthermore, the security personnel can take benefit and they can react to new situations better by replacing the manual methods which consume a lot of time when responding to novel situations. AI-based systems are ready to learn over time and can respond better to threats and attacks. AI help to identify attacks considering the characteristics of application and overall network activity. With the passage of time, AI memorized the normal and regular traffic status and set a limit for the normal activities. Hence, attacked is marked when there is any abnormal deviation.

The development of Artificial Intelligence system requires huge amount of data and input samples. It is evident collecting samples at this amount need lot of time to process and require lot of resources (i.e., memory and processing power etc.). The execution of AI technology requires costly and smart resources. End clients facing challenges in the frequent false alarm. False alarms have destructive effects on the essential responses which lead to disruption of entire business environment.

Fine-tuning, a kind of trade off process, are used to decrease the false alarms and maintain the security level. Intruders and attackers can employ different techniques such adversarial inputs, model theft and data poisoning to target and attack AI-based systems. An AI model comprised of four things such as perception of data, learning, fine decisions, and the ultimate actions. AI systems operating in a very sophisticated environment where all elements must interact and have mutual dependency. For example, a wrong perception can result wrong decision.

Moreover, each of these elements are exposed to different attacks and threats. For instance, decisions are vulnerable to classic cyber-attacks and perception is exposed to training-attacks. Finally, consistency concept is not logical. The prevention of system from misbehaving depends on the elements and these elements should be bounds to maintain lack of certainty. An efficient method is essential to separately verify the decisions, logic fixation and analysis of risk for corresponding elements of AI and ML. To fulfil the expectations of systems and reaction to variety of attacks new techniques are important to implement. The application of AI in cybersecurity area may produce new threats and thus the digital security can be in danger. The consistent detection and prevention of cyber-attacks by AI has also opened doors for attackers to develop more complex threats and attacks.

One of the reason these attackers are motivated because the cost to develop technology decreases when access to AI techniques increases. This is possible that cyber criminals can develop more sophisticated and complex programs with the low amount. The rate of cybercrime has increased due to these factors. The human element of complacency is very important. In AI-based solutions to cybersecurity the risks of human element of complacency are poorly discussed. If institution follow AI and ML methods in cybersecurity, employees could be less conscious of prevention. One of the greatest challenges in AI application in cybersecurity is the collection, management, and processing of unquantified data (structured, semi structured, unstructured, or meta-data) especially when dealing the real-world cybersecurity problems.

This Chapter highlighted the potential applications of AI in the cybersecurity environment. AI providing various opportunities of investigations in the cyberspace. AI is the most effective system to combat against cyber-attacks due to their complexity, number, and flexibility. From the literature reviewed, it's evident that AI-based methods can be employed to resolve cybersecurity issues in a very smart way unlike traditional security methods which are proved ineffective to work in the cyberspace. The continuous research in the AI applications in cybersecurity provide convincing evidence that AI is growing faster in terms of publications and with the passage of time more peoples will be focused on the AI applications in cybersecurity platform. However, the other side of coin should also be considered while talking on the application of AI in cybersecurity. Four important factors which are employed by cyber-criminals must be considered before employing AI in cybersecurity: Adversarial threats, data poisoning and deception, stealing of models and false positive and negative. Despite of these limitations in AI applications, AI open new doors in the cybersecurity research.

Artificial intelligence techniques are vulnerable to adversarial attacks and this is one of the serious issues linked with security of data. AI techniques ignore and skip the traditional software analysis and proposed new attack vectors in the AI algorithms. Many of the applications can affect because of the hidden dependent features. For AI to be used as system element, a depth thorough research is required to develop engineering principles, new theories, and practices. Research required on safety of tools, threats modelling, vulnerability to the environment, and collaboration between human and machine. The designing of such models and techniques should be based on the expertise of AI. These models should repeatedly abstract and refine cyber-attacks. Moreover, the integrity and availability of data, control of data access, operation and privacy of networks, and plastic policy system should be considered.

With the rapid advancements of ICT, new challenges for cyber security have also evolved and emerged. Cyberattacks and threats are now much complex and sophisticated that conventional techniques and approaches are uncapable to help further. These sophisticated cyberattacks need new techniques and approaches which must be ideal, scalable, adaptable, and flexible. In this Chapter Author presented an overview of AI application in the cybersecurity. Some of the well-researched AI-based methods employed in the cybersecurity were discussed such as data learning, security expert systems and bioinspired techniques. Furthermore, areas where AI playing role on cybersecurity are reviewed such as predication, detection, and prevention of intrusion and malware, barriers against

distributed denial-of-service (DDos), a technique where digital police are deployed and many other areas.

The advantages and some of the challenges of AI-based applications in cybersecurity were also discussed. These benefits include handling large volumes of data with high speed and accuracy, reduction in the cost while employing AI techniques in resolving cybersecurity issues and increased ROI on AI powered cybersecurity tools amongst others. Some of the key challenges using AI-based applications for cybersecurity are adversarial machine learning and self-approval by human beings. Nevertheless, AI-based security techniques are still used in the cybersecurity and there are more benefits than disadvantages. As humans are dependent on cybersecurity, many of the industry experts are agreed on the view that AI must be integrated with cybersecurity.