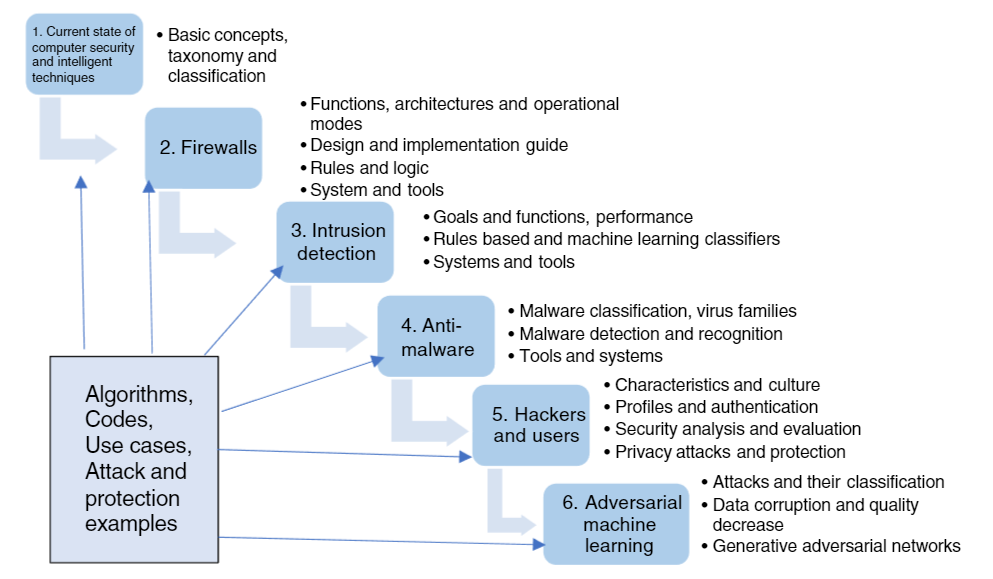
**Flow of Syllabus**

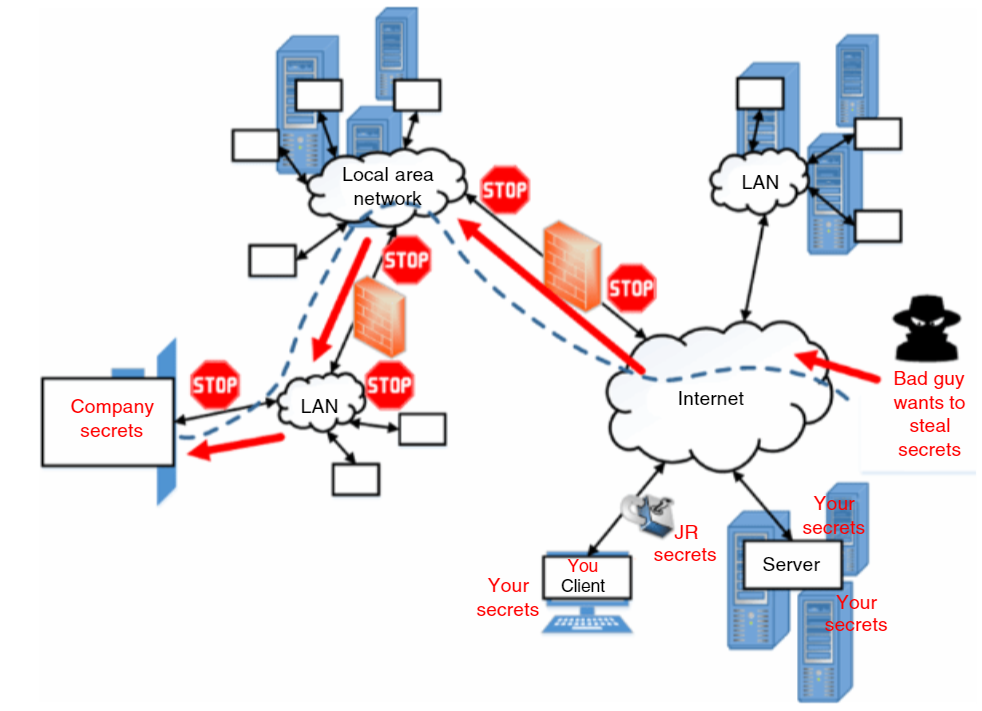


**1.1 The Current Security Landscape**

Computer and network security, also called cybersecurity, is one of the most significant subjects to consider when dealing with computers, networking, and data issues. As data and digital technology gains an inclusion into everyone’s life in general, their security becomes more important too. While more than two billion people are estimated to use the Internet on a regular basis at a present time, the amount of sensitive and private data collected and stored by government and nongovernment organizations that needs to get protected grows up every day. On the other hand, computer systems and communication networks have always been vulnerable to a myriad of threats that can inflict different types of damage resulting in significant losses. The damage can include anything from a data entry error resulting in violation of data integrity to a planted virus that could destroy an entire database with a possible damage source ranging from an outside hacker to an inside mistrusted employee or just a human error.

A new professional community of computer security specialists who are responsible for protecting the systems against adversary attacks and preventing the damage has been formed. Cybersecurity significantly changes the protection landscape and the range of the defense mechanisms. Nowadays, attackers have a wide selection of devices that they could target and infect through local and global networks such as an entire computer infrastructure, mobile phones, and even computerized automobiles. With each passing year, attacks seem to be escalating, also these threats are evolving as attackers invent newer ways to steal, harm, and destroy. Criminals aim at stealing private as well as financial information, and even government and political entities are not immune. Hence, there exist a rising need to safeguard sensitive information and computer resources from these complex and malicious threats. Hacking has been around for decades but present‐day crimes become often not only financially but also politically or personally motivated. The hacker’s activities like identity theft and cyber terrorism create a clear danger to private citizens as well as threats the whole society fabric. The possible hacking sponsorship provided by some government and nongovernment organizations around the world make their ulterior motives and goals even more frightening.

Computer security is a forever evolving field, especially if one takes into account the current technological and societal developments. Two major interrelated trends are observed in a modern technological development: computerization or digitization and interconnection through the Internet (Figure 1.1).



Over the last couple of decades, the number of devices connected to the Internet has grown at a large scale. New computerized products, which are released nowadays have an Internet connection capability, and the rate at which they utilize it is high. These devices generate and collect an astronomical amount of data, which needs to be stored, processed, communicated, and accessed However, with time, more and more complex exploits get built.

The computer security has always been a quintessential aspect when it comes to technology. The security has grown stronger in comparison to how it looked a few decades ago but so have the threats. New kinds of threats and attackers have been coming up and testing the resistance of the computer and information systems since then (Figure 1.3). Now, with the wide number of many electronic gadgets such as mobiles and any data storage devices, and also with an immense adaptation of computer technology in all kinds of diversified sectors, the need for the sound security control mechanisms and tools grows faster than ever before too. Initially, attackers targeted the large‐scale organizations in financial sectors but it has changed. Nowadays, they are coming after smaller organizations too. Attackers are looking for any form of assets to steal or modify, they can get an access to.

A diagram of a graph

Description automatically generated

Big data and pervasive computing are the new areas, which cyberattackers set up to exploit. Mobile phones, tablets, and laptops compose the areas, which are most vulnerable. Immense research is carried out in these fields to make them secure. Not long time ago, the picture looked different. There were limited number of devices and the Internet was not so widespread. Cloud computing was a concept only. Not all the data were stored in the cloud. The viruses were not smart enough to exploit the available vulnerabilities. Nor had the hackers tools so powerful, that people with limited or no knowledge of computing could actually get into systems of other owners. Figure 1.3 demonstrates the growth in attacks diversity and sophistication and at the same time the decrease in the knowledge possession required for conducting cyberattacks due to the availability of automated tools.

**The major reasons that are commonly given to explain the growing cost of cybercrime are:**

●quick adoption of new technologies by cyber criminals,

●the increased number of new users online, who nowadays mostly come from low‐income communities and countries with weak cybersecurity education and implemented protection mechanisms,

●an increased ease of committing cybercrime, with the growth of cyber‐crime‐as‐a‐service development and criminals attempting to monetize their breach success,

●an expanding number of cybercrime centers around the world that might get supported by their government agencies,

●a growing financial sophistication among top‐tier cyber criminals and availability of cryptocurrencies that, among other things, make crime monetization easier.

Just some recent data. M‐trends (2020) reports that in 2019, Mandiant professionals observed that attacks:

●7% originated with or used compromised third‐party access,

●15% had multiple attackers,

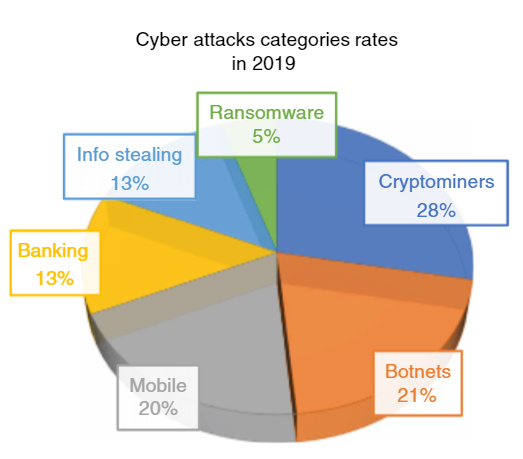
●less than 1% involved an insider,

●22% had data theft likely in support of intellectual property or espionage end goals,

●29% were likely for direct financial gain including extortion, ransom, card theft, and illicit transfers,

●3% of these targeted attacks were for the purpose of reselling access gained in the intrusion,

●4% likely served no purpose except for creating compromised architecture to further other attacks.



**1.2 Computer Security Basic Concepts**

An attack is the basic term in computer security. It can be described as an offensive intent to disrupt confidentiality, integrity, and availability of data associated with a protected computer’s infrastructure. Cyber or computer security goal is defined as a protection of those important assets against all possible attacks. It may include the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance mechanisms, and technologies that can be used to protect the cyber environment and organization’s as well as user’s assets.

In today’s world of pervasive computing, where there is a need for accessing the Internet and an immensely large number of interconnected networks, the vast amount of data is being shared. Not all the information and data out there should be open for everyone, quite to the contrary, a big chuck should be held private with a very limited access from authorized users only. It is important to keep the data safe and secure.

Computer security approach integrates three major concepts (see Figure 1.6) according to the formula:

**Computer security = Confidentiality plus Integrity plus Availability**

**A diagram of a computer security

Description automatically generated**

**A white text on a black background

Description automatically generated**

**1.3 Sources of Security Threats**

Following organizational, technological and human factors have been identified as the main causes of attacks on computer security.

**1) Weakness in the computer and network infrastructure and protocols**

A computer network provides connectivity to the group of computers connected together. For any individual, group, or organization, information/data represents the key asset and becomes the core for their future growth with respect to analysis and planning. The various types of fragility’s toward security of computer and network systems can be found at the various levels.

**Policy level weakness**

A computer security policy defines the goals and elements of an organization’s computer systems and networks. Security policies are very important for organizations that keep a track of data flow through the network. Security risks exist if the policies are not followed or if there are no strictly defined guidelines. A security policy must meet certain goals. Among others, it must state how to audit or configure the systems to verify whether the system follows the network policy, it should specify the steps through which requirements are met and finally it should provide proper guidelines to the staff and users for protecting the information and resources. If certain important areas are not covered or misunderstood, the security mechanisms that are set up based on the policies might have loopholes in organization system protection.

**Technological weakness**

depends on technical factors and solutions such as chosen network and communication equipment, protocols, and operating systems. Using certain older protocols, for example, telnet might result in weakening security as hackers might get a better chance to exploit the vulnerabilities in the computer systems.

**Configuration weakness**

It might result in unauthorized accounts, unsecured settings, and misconfigured network equipment. All of these factors may lead to vulnerabilities, which could be captured and exploited by the hackers.

Besides the policy itself, the security level depends on its implementation and other factors listed below.

**2) Design and implementation problem**

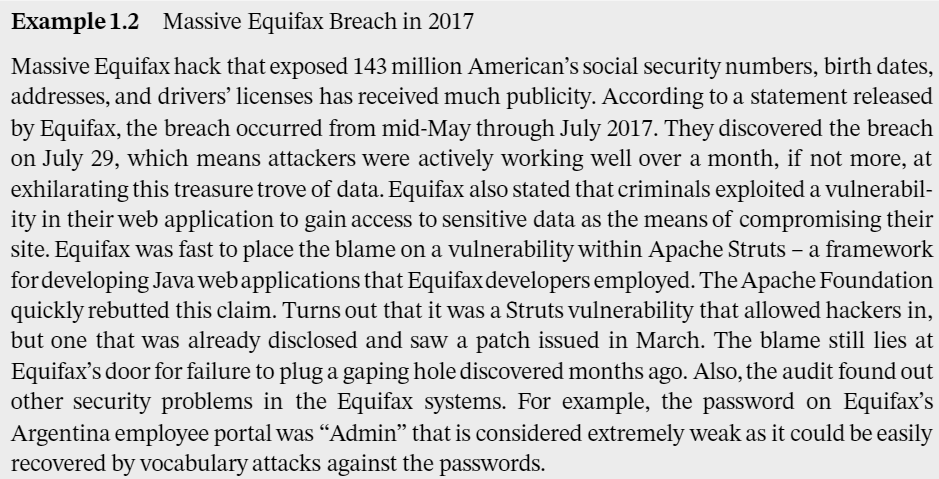
may include inadequate logging of security relevant events, incorrect or incomplete access controls, insecure default setup conditions, and failure to address security issues from external sources.

A close-up of a text

Description automatically generated

**3) Vulnerabilities in software systems and tools**

A decade ago, vulnerabilities were usually found by a criminal and then incorporated into their attacks. A few years ago, it became much more common to see professional teams of criminals who discovered and developed attack software. The current trend builds up an overlap between criminal developers and the advanced persistent threat (APT), or nation‐state actors, to create a steady stream of zero‐day tools targeting specific organizations and individuals (State of Internet/Security 2019). Unfortunately, even after the vulnerabilities have been reported and the patch has been released, the discovered vulnerabilities might remain unpatched for a long time, creating an opportunity for their malicious exploitations. 85% of the attacks observed by Check Point global attack sensors in 2019 leveraged vulnerabilities registered in 2017 and earlier (Checkpoint 2019).



**4) Hackers’ activity:** that might include setting up fake wireless access points, access to cookies in a browser, password cracking, etc.

A close-up of a text

Description automatically generated

A close-up of a document

Description automatically generated

**5) Social engineering**

Social engineering is the art of manipulating people to make them give up confidential information. The attackers may try to access different types of information. They may, in some way, ask for passwords indirectly, obtain one’s bank account information, and install malicious software on someone’s computer. Many times, a computer user does not even understand that some-

thing wrong is going on. These attacks are common because the users cannot discriminate between real and fake parties on the web. The most common attack of this type is phishing, in which an attacker poses as a legitimate party. For example, in this type of attack, the attackers create a fake web page that looks very similar to the original one.

Suppose, the attacker creates the web page that looks almost the same as the web page of a bank, the users may not notice anything malicious and enter all their details on the page. Now, the attacker gains access to all login information and this information may be used to get access to the real online banking page. There is another very popular attack, in which hackers send emails to users that contain exciting offers. Many users get tricked and simply click on the link. After user’s clicking, the attackers ask for user’s bank details or the social security number and other important details. Users get tempted by the offer and enter their details and thus compromising on private information. There are some other modifications (Security Tip 2020). For example, Vishing

is the social engineering approach that leverages voice communication. This technique can be combined with other forms of social engineering that entice a victim to call a certain number and divulge sensitive information. Advanced vishing attacks can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity (ID) to be spoofed. This attack can take advantage of the public’s misplaced trust in the security of phone services, especially landline services. Landline communication cannot be intercepted without a physical access to the line. However, this trait is not beneficial when communicating directly with a malicious actor.

**Smishing**

is a form of social engineering that exploits SMS, or text messages. Text messages can contain links to such things as webpages, email addresses, or phone numbers that, when clicked, may automatically open a browser window or email message or dial a number. This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious attacks.

One other recent kind of attack is related to social networking sites. There could be some pages on Facebook, which tempt one to open them. Some of them are like “Find who is your best friend,” “When will you get married.” These applications, when opened, gain access to one’s profile by saying that it needs to analyze the profile to answer the above questions. After processing the responses, these applications have all information on Facebook. They may be able to get one’s password, and then make posts on one’s account, which may look like the owners themselves posted it. The attackers may post some other links on someone’s wall and so the friends then click on them and the cycle continues.

**Suspicious sender’s address,**

which, however, may imitate a legitimate business one. Cybercriminals often use an email address that closely resembles one from a reputable company by altering, or adding and omitting a few characters.

**Generic greetings and signature**

such as “Dear Valued Customer” or “Sir/Ma’am” and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address the recipient by name and provide their contact information.

**Spoofed hyperlinks and websites.**

If one hover the cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g. .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.

**Spelling and layout**

that may include poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.

**Suspicious attachments.**

An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.

**6) Physical theft**

Despite being very old, the physical theft is still considered as the second most seen computer security threat, after malware infection. It is one such part of computer security, which many people do not take into consideration. The mobile phones, laptops contain huge amount of data that are useful for the user and should be kept private. Such kinds of devices are easy to steal because of their size. There is a huge market for independent parts of such devices because of their widespread use. For organizations, even a loss of one laptop may have a huge impact. The devices usually contain personal information of employees or customers, confidential product information, confidential strategic information about business, or other sensitive information. This does not apply to laptops only, other types of devices like flash drives, discs, mobile phones, and tablets are vulnerable to theft as well. Many users believe that even if a laptop is stolen, the thief would not be able to access their data because the user has set a login password. But there are multiple ways, in which the attackers could obtain an access into the system. After gaining an access, they can access all saved passwords from the browsers and could cause a lot of trouble.

**1.4 Attacks Against IoT and Wireless Sensor Networks**

In a growing trend of mobile computing penetration and usage, IoT devices, often composed into wireless sensor networks (WSN), offer a cheap and distributed means of gathering data. They usually operate autonomously or through various managed clusters. Limited resources of energy (usually a battery, or a solar panel generating very little energy), storage and computing capacity of IoT devices make them vulnerable targets to a variety of attacks designed to either capture the nodes, cripple, and/or disrupt their normal operation. Traditional methods of communication and security (prevention via cryptographic means, detection, and reaction, among others) cannot be employed in these devices in their present conventional form, since the requirements of these methods are not (for the most part) designed to operate within severely limited resource constraints. Therefore, some modifications and ingenuity are required in order to secure these nodes and networks despite their shortcomings, with methods that have a positive track record in their respective conventional realm.

The greatly sought commodity of mobility afforded from this technology in computing and communications will, in all likelihood, increase with time as the technology matures and is deployed more widely. Unfortunately, this progress will likely be accompanied by attack numbers increasing. The ways to ensure their security (both via prevention, and especially early detection) is an aspect that is quite essential. It would not take a lot of resources to mount a successful attack against the IoT devices and networks.

Attacks on IoT take shape in two forms – physical and cyber. The former deals with physically impeding the devices to function, whether it be capturing or damaging the devices, or destroying the hardware itself. The nonphysical aspect is when the adversary cannot physically access or is not interested in capturing the devices, but rather wants to either render them useless in terms of operating within designed parameters, or sniff out the information.

**1.4.1 Preliminary and Simple Attacks**

Below are the attacks examples that have been investigated and employed.

**Passive Information Gathering** attack sniffs communication as it is being transmitted between devices. This takes the form of collecting information without doing any alterations to the data, so it might be considered as an attack against confidentiality. This approach does not intrude or degrade the communication signals, thus it is effective and non-invasive. Since it is passive, there is no way of knowing whether someone is sniffing and collecting data. It is important to protect the content, given the broadcast nature of the IoT communication. To counter this attack, a simple use of encryption and access control mechanisms will suffice. This way, the adversary would not be able to read the data being transferred, nor gain access to receive any data without authorization.

**Traffic and Node Activity Analysis** involves gathering of information on IoT activities and traffic patterns. It is similar to Passive Information Gathering attack in that it is nonintrusive too and frequently follows up it. This attack is primarily used for future attack preparations to follow up after sufficient information has been collected to extract patterns of communication and its contents. Countering this attack is possible in the similar fashion as with the previous attack – by using encryption and access control enforcement mechanisms.

**Device(node) Subversion by Tampering or Destruction** targets at capturing or destroying the physical device(s), with the aim of collecting information available including encryption/decryption keys (if applicable), credentials to access the network, or just simply take out the hosts that make up the wireless network, respectively.

Protection from this attack could take the form of physical protection of the hardware and access control to alleviate any access to information. The former is a bit tricky – if the cost of the device is low, then it makes no sense to physically protect them from the adversary. However, access control is still important in that it protects the network by restricting who and what has access to a node, and potentially, network information.

**Device (node) Malfunctioning** could happen for a variety of reasons, and not necessarily through an attack, so there is no way to know whether the cause was malicious, the hardware failed on its own, or a natural occurrence (such as a squirrel chewing on the device, rain short‐circuiting the logic boards, etc.) incapacitated the devices. The symptoms usually take the form of generating inaccurate data or violating traffic/routing protocols/rules. There is no particular way one can detect whether it is an attack or not, thus the only thing that can be done is to perform tests on the hardware (if the device is still online) and see if the diagnostics pass.

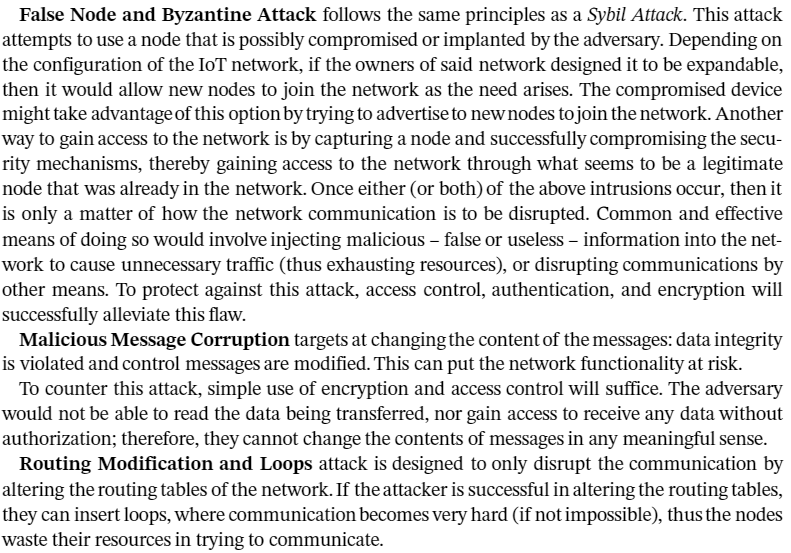
**Cluster Leader or an Aggregate Node Outage** may happen for a variety of reasons as in a previous case. The symptoms are similar as well, including the generation of inaccurate data or violating traffic/routing properties. The remedy to this is doing flexible network structuring and rerouting of traffic to avoid the affected area.

**1.4.2 Active Attacks**

These attacks commonly employ more sophisticated methods; instead of passively sniffing traffic or physically tampering the nodes, they focus on making the communication hard or impossible to take place, making sensors supply the wrong values, etc.

**Sensor Stimuli** targets the sensed readings as a tool to help with resource exhaustion. The prerequisite of this attack is to have a subverted node – this way, said node can send requests to the network (and as a result, other nodes) for further sensor readings. The repeated requests will  eventually exhaust the resources of the node. To stop this attack, the usual arsenal of access control and encryption mechanism is employed.

**Sybil attack.** It is similar to sensor stimuli attack, but goes a step further in sophistication. The aim of this attack is to disrupt the communication, though not in a primitive form of a denial of service attack. What this attack attempts to do is to clone a node or nodes and to try to corrupt and/or disrupt the routing information to and from other nodes. This causes traffic to become congested or completely disrupted. Unnecessary traffic sent to build/repair routing tables etc. Basically, disruption of the flow of both control and actual information from being able to move around to the appropriate destinations. As with the previous few attacks, the counter measures are simple enough to implement – an access control/authentication mechanism and encryption. This will prevent a node from being impersonated.



A close-up of a document

Description automatically generated

A close up of a text

Description automatically generated

A close-up of a text

Description automatically generated

A close-up of a document

Description automatically generated

**1.5 Introduction into Artificial Intelligence, Machine Learning, and Data Science**

**A close up of a text

Description automatically generated**

**A close-up of a text

Description automatically generated**

**A close up of text

Description automatically generatedA close up of text

Description automatically generated**

**A timeline of history of the past

Description automatically generated with medium confidence**

**Cyber security has become a significant part of the big data phenomenon, where the volume of available data, the velocity of its generation, the variety of various data sources and the data veracity and quality problem scale move cyber security out of the human abilities range.**

**To address those challenges. Unfortunately, this discrepancy between cyber security problems, sophistication, volume and variety on one hand and the human operator qualification to address them on another is expected to grow up even much more.**

**Analysing and improving cyber security posture is not a human scale problem anymore.**

**Cyber criminals and hackers have realised it and have been already widely utilising intelligent techniques and technologies.**

**Cyber security professionals, in order not to lose in the competition, have to employ intelligent technologies too. Fortunately enough, they have had already gained a lot of experience in design and application of intelligence systems, in enhancing network security, recognising attacks, discovering security vulnerabilities and differentiating legitimate users from hackers.**

**In cyber security practice most of the existing tools employ ai in one form or another however those applications remain more or less hidden.**

**Various AI definitions do exist. Even ISO (the International Organization for Standardization) attempted to provide 2 definitions as:**

1. **An interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning.**
2. **The capability of a functional unit to perform functions that are generally associated with human intelligence, such as reasoning and learning.**

| **Feature** | **Rules-Based Systems** | **Expert Systems** |
| --- | --- | --- |
| **Rule Representation** | **Uses explicit "if-then" rules, where conditions trigger specific actions.** | **Knowledge base contains facts, rules, and heuristics to emulate human expertise. Rules may also be in "if-then" format.** |
| **Inference Engine** | **Applies rules to data or inputs using a straightforward inference engine.** | **Utilizes an inference engine that processes the knowledge base, employing various reasoning methods like forward chaining or backward chaining.** |
| **Knowledge Base** | **Primarily consists of rules that define conditions and actions.** | **Knowledge base includes facts, relationships, and inference mechanisms, capturing expert knowledge in a specific domain.** |
| **Scalability** | **Can become complex as the number of rules increases. Managing and updating large rule sets may require careful organization.** | **Complexity is handled through the organization of knowledge in the knowledge base. The system can handle a large amount of expert knowledge.** |
| **Transparency** | **Rules are explicit and easily understandable, providing transparency in decision-making.** | **Transparency in decision-making is maintained through explicit representation of expert knowledge in the knowledge base.** |
| **Learning and Adaptation** | **Learning mechanisms are typically limited; the system relies on predefined rules.** | **Can be designed with learning mechanisms to refine knowledge and improve performance over time. Learning may involve updating the knowledge base based on feedback or new data.** |
| **Complex Problem Solving** | **Suited for problems with well-defined conditions and actions.** | **Designed for complex problem-solving tasks within a specific domain. Can handle uncertainty, incomplete information, and ambiguous situations.** |
| **Applicability** | **Commonly used in business rules, workflow automation, and decision support systems.** | **Applied in areas such as medical diagnosis, financial analysis, troubleshooting, and other domains where specialized expertise is crucial.** |