Information Security: A General Overview

Boyuan Zheng

Abstract—Information security, often abbreviated InfoSec, is usually defined as the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Its primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad). The history of Information security can date back to the Caesar cipher in the 17th century. Since the invention of computers and the subsequent popularity of the Internet, information security technologies kept evolving in defense of the development of viruses and cyber attacks. Nowadays, with common threats like MitM attack, APT and DDoS happening day in and day out, the importance of information security has gained more and more attention. With technologies such as SIEM, PKI, etc. in recent use, information security plays an important role in such fields as disaster recovery, vulnerability management and so on. In the near future, the emergence of technologies such as big data, artificial intelligence and blockchain not only bring challenges to the field of information security, but provide new development directions and opportunities. This report provides a general overview on the development and history of information security, introducing its popular technologies, applications and trend of developing in prospect.

Index Terms—Information Security, Computer Security, CIA

1 Introduction

Information security, often abbreviated InfoSec, is usually defined as the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users [1]. It's part of information risk management and involves preventing or reducing the probability of unauthorized access, use, disclosure, disruption, deletion, corruption, modification, inspection, or recording. Information security encompasses physical and environmental security, access control, and cybersecurity. The information it protects comes in many forms, whether it is electronic or physical, tangible or intangible.

The core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise [2]. The CIA triad makes up the cornerstones of strong information protection, creating the basis of security infrastructure.

In recent years, the field of information security has been greatly developed. However, despite growing awareness of information security issues and the proliferation of cybersecurity technologies, the total number of reported breaches continues to grow at an alarming rate. Information security threats come in many different forms, of which some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of devices or information, sabotage, and information extortion. As knowledge has become one of the most important assets in the 21st century, the efforts to protect information security have correspondingly become more and more important, and the field of information security is booming accordingly.

• *Boyuan Zheng is with the Department of Computer Science, Tongji University, Shanghai, China.*

1.1 The CIA Triad: Three Pillars of Information Security

First mentioned in a NIST publication in 1977, The CIA triad of confidentiality, integrity, and availability is considered as the key concepts of information security. The three members of the triad are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.

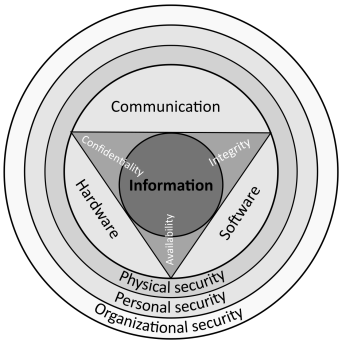

Fig. 1: Information Security Attributes : Confidentiality, Integrity and Availability (CIA)

1.1.1 Confidentiality

The ISO 27001 standard describes confidentiality as "the property, that information is not made available or disclosed to unauthorized individuals, entities or processes." Confidentiality mechanisms range from physical access controls (e.g., guards, gates, guns) to system and network authentication and authorization tools, to data encryption mechanisms. Confidentiality guarantees are usually enforced by a number of mechanisms including authentication and authorization, encryption and the related notion of key management and data life cycle management [3].

1.1.2 Integrity

Information integrity is the maintenance and assurance of the accuracy and consistency of information over its entire life cycle. Information is said to maintain integrity if it is recorded exactly as intended and upon later retrieval, is the same as it was when it was originally recorded. Integrity means that unintentional or unauthorized changes to information are prevented.

1.1.3 Availability

Information is useful only insofar as it is available when required. This means that the computing systems used to store and process the information, the security controls used to protect it and the communication channels used to access it must function properly. Systems requiring high availability assurance must design for unexpected disruptions such as power outages, hardware failures, anticipated downtime associated with system upgrades and malicious activity such as denial-of-service attacks.

1.1.4 Other Key Concepts

Though the CIA triad is widely applied, debate continues about whether or not it is sufficient to address rapidly changing technology and business requirements, with recommendations to consider expanding on the intersections between availability and confidentiality, as well as the relationship between security and privacy. Other principles such as **authenticity** and **non-repudiation** have sometimes been proposed as a complement.

Authenticity - refers to the notion that the party being communicated with is really who they claim to be, with respect to information security. Many techniques are used to ensure this, such as pre-shared keys, public/private key algorithms, and, recently quantum cryptography.

Non-repudiation - refers to guarantees that the author of a statement will not be able to successfully challenge his or her authorship of the statement or validity of an associated contract execution. It can be achieved through a service that provides proof of the integrity and origin of the information and high levels of assurance with respect to authenticity.

1.2 Common Information Security Threats

There are various forms of threats to information security, with thousands of them happening everyday. The following lists some common information security threats.

1.2.1 Advanced Persistent Threats (APT)

APTs are threats in which individuals or groups gain access to your systems and remain for an extended period. Attackers carry out these attacks to collect sensitive information over time or as the groundwork for future attacks. APT attacks are performed by organized groups that may be paid by competing nation-states, terrorist organizations, or industry rivals.

1.2.2 Distributed denial of service (DDoS)

DDoS attacks occurs when an attacker overloads a server or resource with requests. Attackers can perform these attacks either manually or through a botnet, a network of compromised devices used to distribute request sources. DDoS attacks are designed to prevent users from accessing services, or to distract security teams in the event of another attack.

1.2.3 Social Engineering Attacks

Social engineering involves using psychology to trick users into providing information or accessing attackers. Phishing via email, is a common form of social engineering. In a phishing attack, the attacker pretends to be a trusted or legitimate source, asking for information or warning the user that action needs to be taken. If the user complies, the attacker can access credentials or other sensitive information.

1.2.4 Man-in-the-middle (MitM) attack

MitM attacks occur when communications are sent over insecure channels. During these attacks, attackers intercept requests and responses to read the contents, manipulate the data, or redirect users. They may secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other [4].Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority.

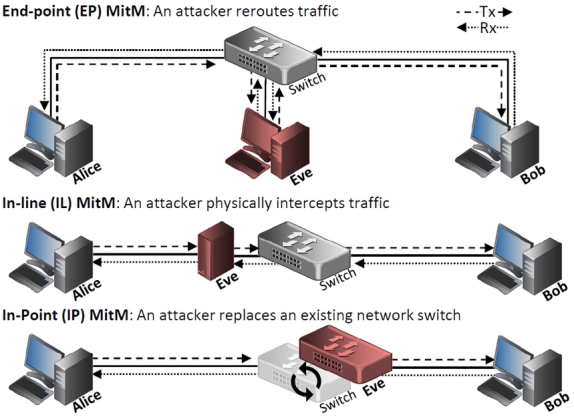

Fig. 2: Different types of MitM

1.2.5 Ransomware

Ransomware attacks use malware to encrypt your data and hold it for ransom. Attackers usually demand information, demand some kind of action, or demand that an organization pay a ransom in exchange for decrypting data.It s a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In

a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

Ransomware attacks are typically carried out using a Trojan disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the WannaCry worm, traveled automatically between computers without user interaction.

1.2.6 Virus, Worm & Trojan Horse

Viruses, worms and trojan horse in common damage the confidentiality and integrity of computer information and destroy information security. But they also have their differences, which can be seen below.

A **Computer Virus** - is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses.Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage.

A **Worm** - is a type of malicious software that can spread itself by exploiting vulnerabilities in the operating system and other related vulnerabilities. It can be spread over the Internet, automatically spreading from one computer to another, and on each computer performing a computer-threatening operation. When the malware is started, it will damage the user's computer system and data files, such as deleting system files and formatting hard disk data. Although both worms and viruses are capable of self-replication and propagation, compared with viruses, worms do not need to rely on host programs and can run independently by themselves [5]. When worms spread through a network on a large scale, they rapidly consume network resources and cause network congestion. Creeper is believed to be the first worm in computer history, which will be covered in more detail later in the history part.

A **Trojan Horse** - is any malware that misleads users of its true intent. The term is derived from the Ancient Greek story of the deceptive Trojan Horse that led to the fall of the city of Troy. Trojans generally spread by some form of social engineering; for example, where a user is duped into executing an email attachment disguised to appear innocuous (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller who can then have unauthorized access to the affected computer. Ransomware attacks are often carried out using a trojan. Unlike computer viruses, worms, and rogue security software, trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves [6].

1.3 Strategies of InfoSec

1.3.1 Cryptography

The word cryptography means "secret writing." Some define "cryptography" as "study of mathematical techniques". It plays some multiple roles in user authentication. Cryptographic authentication systems support authentication capabilities through the need of cryptographic keys known or consumed only by authorized entities. Cryptography also provides authentication through its extensive use in other authentication systems.

Password systems apply cryptography to encrypt stored password files, card/token system apply cryptography to secure sensitive stored data, and hand-held password generators often apply cryptography to make random, dynamic passwords.

Cryptography is generally used in distributed applications to transfer identification and authentication data from one system to another over a network. Cryptographic authentication systems authenticate a user depends on the awareness or possession of a cryptographic key. Cryptographic authentication systems can be depends on private key cryptosystems or public key cryptosystems.

Private key cryptosystems need the same key for the functions of both encryption and decryption. Cryptographic authentication systems depends upon private key cryptosystems based upon a shared key between the user attempting access and the authentication system.

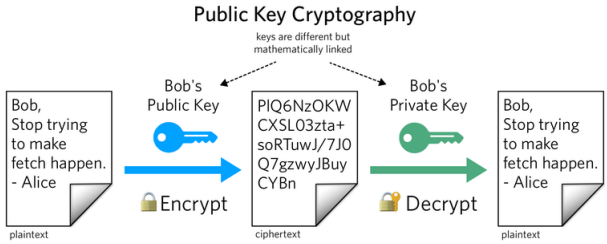

Fig. 3: Public Key Cryptography

Public key cryptosystems separate the functions of encryption and decryption, generally using an independent key to control each function. Cryptographic authentication systems depends upon public key cryptosystems based upon a key known only to the user attempting access.

1.3.2 Access Control

In computer security, general access control includes authentication, authorization, and audit. A more narrow definition of access control would cover only access approval, whereby the system makes a decision to grant or reject an access request from an already authenticated subject, based on what the subject is authorized to access. Authentication and access control are often combined into a single operation, so that access is approved based on successful authentication, or based on an anonymous access token. Authentication methods and tokens include passwords, biometric analysis, physical keys, electronic

keys and devices, hidden paths, social barriers, and monitoring by humans and automated systems.

The requirements for using—and prohibitions against the use of—various system resources vary considerably from one system to another. For example, some information must be accessible to all users, some may be needed by several groups or departments, and some may be accessed by only a few individuals. While users must have access to specific information needed to perform their jobs, denial of access to non-job-related information may be required. It may also be important to control the kind of access that is permitted (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken. Access is the ability to make use of any system resource.

Examples of access control security controls include: account management, separation of duties, least privilege, session lock, information flow enforcement, and session termination.

1.3.3 Defense In Depth

Defense in depth is a strategy that leverages multiple security measures to protect an organization's assets. The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way. Defense in depth addresses the security vulnerabilities inherent not only with hardware and software but also with people, as negligence or human error are often the cause of a security breach.

Today's cyber threats are growing rapidly in scale and sophistication. Defense in depth is a comprehensive approach that employs a combination of advanced security tools to protect an organization's endpoints, data, applications, and networks. The goal is to stop cyber threats before they happen, but a solid defense-in-depth strategy also thwarts an attack that is already underway, preventing additional damage from taking place.

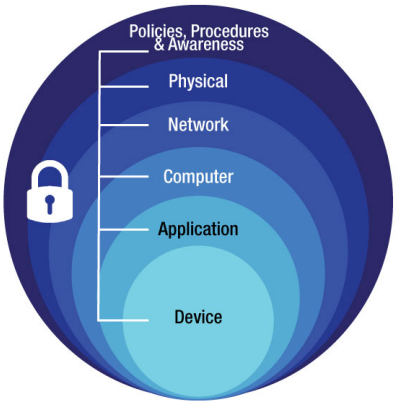

Fig. 4: Defense-in-depth Layers

Antivirus software, firewalls, secure gateways, and virtual private networks (VPNs) serve as traditional corporate network defenses and are certainly still instrumental in a defense-in-depth strategy. However, more sophisticated measures, such as the use of machine learning (ML) to detect anomalies in the behavior of employees and endpoints, are now being used to build the strongest and most complete defense possible.

2 History

The history of information security began long before the rise of the telegraph, wireless or the Internet. Its origins can be traced back to the hierarchical command and control structures that emerged in ancient civilizations in administration and warfare [7].

2.1 Ancient Times: The Caesar Cipher

Ancient cultures, including the Greeks, Romans and Hebrews, used simple substitution codes for diplomatic and military communication. Historically, Julius Caesar is considered the creator of the most basic type of substitution cipher. The Caesar Cipher, named after him, was invented in January 1684 during the war between the Dutch Republic and France. A Caesar cipher encodes a message by moving the alphabet by a predetermined number of letters and replacing each letter in the message with a new letter.

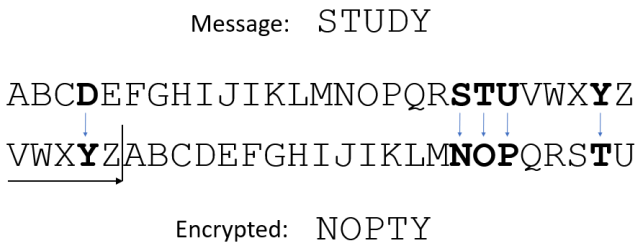

Fig. 5: A Caesar substitution cipher with a shift of 5 letters

2.2 During World War II: The Enigma Machine

Cryptography took a big leap forward in the early 20th century with the invention of mechanical rotor machines, among which the most famous one was the Enigma used by the Germans during World War II [8]. The decryption of the Enigma messages by Allied codebreakers is considered to have played a huge role in defeating the Germans and is recognized as one of the turning points in the history of information security. The information age, when the first computer entered human life after the Second World War, also introduced the concept of information security. Instead of storing information and communicating over the Internet, as they do today, computers emerged primarily as products of encryption.

2.3 The 1970s: The ARPANET and Creeper

In the 1970s, The Advanced Research Projects Agency Network (ARPANET) marked the beginning of the true birth of

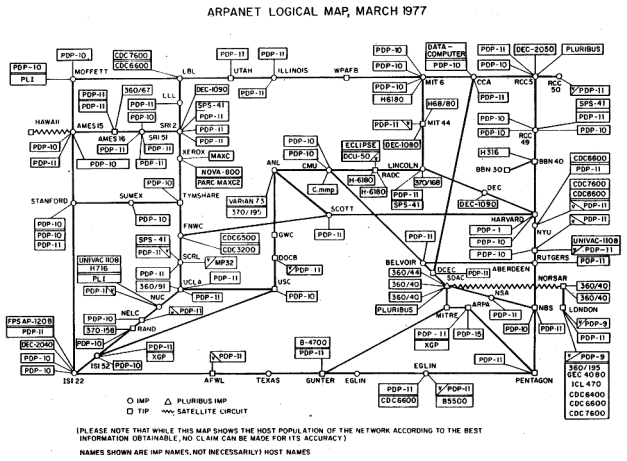

Fig. 6: ARPANET logical map

cybersecurity. ARPANET was the network developed prior to the internet, and was very important to understand the coverage area and the scale of the concept of information security. In the early years of the ARPANET, the US Department of Defense commissions a study that's published by the Rand Corporation as Security Controls for Computer Systems. It identifies many potential threats and possible security measures. Known as the Ware Report, this report becomes influential to security certification standards and processes. According to the IEEE Annals of the History of Computing, it marked the start of the field of computer security [9].

Creeper, a computer program which was able to move ARPANET's network and leave a small trail wherever it went, was created by a researcher named Bob Thomas. It was then taken to the next level, as Ray Tomlinson making it self-replicating and the first ever computer worm. He then wrote another program called Reaper which chased Creeper and deleted it, widely regared as the first example of antivirus software.

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19   3 JOBS
LOAD AV   3.87   2.95   2.14
JOB TTY  USER      SUBSYS
1   DET  SYSTEM    NETSER
2   DET  SYSTEM    TIPSER
3   12   RT        EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Fig. 7: Creeper: the first computer worm

the Creeper and Reaper served a highly important purpose, revealing a number of flaws in ARPANET's network security. They have raised huge concern at the time, as many large organisations and governments were linking their computers via the telephone lines to create their own networks. On the other hand, certain groups of people began to recognize this as well, seeking out ways to infiltrate these lines and steal important data.

2.4 The 1980s: The Morris Worm and the Viral Era

During this time, the use of the web began to expand rapidly, with more universities, militaries and governments connecting to it, meaning that the security measures needed had to gradually become more extensive as well. As computers become more connected and computer viruses become more advanced, information security systems can barely keep up with the ever-increasing number of innovative hacking methods.

The birth of the Morris worm in 1988 was an important turning point in the history of information security. The worm, named after its inventor Robert Morris, is designed to spread across networks, exploit known vulnerabilities to infiltrate terminals and then replicate itself. The aim is to identify the inadequacies of network intrusion prevention systems. The worm replicates so quickly that it incapacitates the target computer and slows the Internet to a crawl. It also spread quickly across the network, causing untold damage.

After the Morris worm, viruses began to become more and more deadly, affecting more and more systems. This worm seems to herald the age of the massive Internet outages we live in. Meanwhile, the Morris worm helped fuel the rise of anti-virus software as a commodity - the first dedicated antivirus company was born in 1987.

2.5 The 1990s: The Rise of Firewalls

With the invention of the World Wide Web in 1989, more and more people began to put their personal information online. Because of this, organized criminal entities saw it as a potential source of revenue and have begun to steal data from people and governments via the web.

By the mid-1990s, cybersecurity threats were growing exponentially, so firewalls and antivirus programs had to be mass-produced to protect the public. Firewall, originally referred to a wall intended to confine a fire within a line of adjacent buildings, is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules in computing [10]. It typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

However, while these firewalls and antivirus programs have reduced the risk of attacks to some extent, computer viruses and worms continue to appear, so attacks by hackers are still rampant and hard to prevent.

2.6 After the 2000s: InfoSec Moving Forward

In the early 2000s, despite increased sentences, cybercriminals continue to use their skills to remain anonymous and successfully infiltrate computer networks and operating systems. As a result, prevention through online security, rather than relying on the threat of jail time is necessary.

Though emerged since the 1970s, data encryption has provided a secure way to prevent unauthorized access since the 2010s. Encryption scrambles the data and makes it unreadable to hackers, thus protecting not only the network, but also individual digital files during storage and data transfer. More and more organizations are developing and implementing information security policies to ensure that employees follow best practices to prevent data breaches of data management systems and archives.

While serious information security incidents like Wannacry ransomware worm is still happening, there are more and more companies offering solutions to these potential tragedies. Information security is constantly improving, and many companies are designing a large number of novice attack mitigation options utilizing Network Behavior Analysis (NBA), Web Application Firewall (WAF), and Denial of Service (DoS) protection.

3 Technologies

3.1 Firewall

A firewall is defined as a "component or set of components that restricts access between a protected network and the Internet, or between other sets of networks." [11] Firewalls are network security resources that are defined to control the flow of data between two or more networks. From a high-level perspective, they can serve as a choke-point, designed to restrict, or choke, the flow of network traffic, or as a gateway that performs further processing on the traffic beyond simple choking restrictions.

Also, many firewalls provide capabilities like Network Address Translation (NAT) that provide a logical separation between networks by changing the underlying numbering scheme (IP addressing). NAT is an important feature because it allows organizations to interconnect their resources internally using IP address space that is reserved for internal use by RFC 1918. This reserved space is not routable on the Internet, and thus is not directly accessible to attackers outside the firewall performing the NAT.

3.2 Security Information and Event Management

Security information and event management (SIEM) systems first became available in the nineties and were adopted by security operations centers because of their promise to provide insights into the deep, dark corners of their networks. Information security teams can use SIEM to know when and where security threats are occurring in order to investigate these incidents and make decisions about appropriate responses.SIEM systems have a history of more than 15 years, and traditionally combine comprehensive security approaches into a management solution, including:

Log management system (LMS) - A procedure for simple collection and centralized storage of logs.

Security Information Management (SIM) - A tool that automatically collects log files for long-term storage, analysis, and reporting of log data.

Security Event Management (SEM) - Technology for real-time monitoring and correlation of systems and events, with notifications and console views.

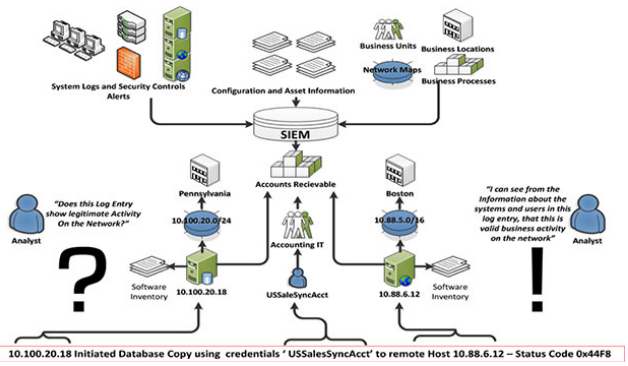

Fig. 8: Security information and event management system

3.3 Intrusion Detection and Analysis System

As early as 1980, the concept of intrusion detection appeared [12]. In its most basic form, intrusion detection is designed to detect the misuse or abuse of network or system resources and to report such instances. The following sections discuss each of these technologies and provide an overview.

3.3.1 Intrusion Detection Systems (IDS)

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Intrusion detection systems are typically classified according to their primary method of detection: network-based, host-based, hybrid, or network-node. Network-based detection captures packets directly off the network, while host-based detection resides on a host and captures data as it flows into and out of that host. Hybrid systems aggregate the capabilities of network-based and host-based systems whereas network-node systems try to function like a network-based system while residing on a host.

3.3.2 Intrusion Prevention Systems (IPS)

Intrusion prevention systems, or IPS, are often defined as "any device (hardware or software) that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful." IPS have grown from a desire to combine the deep inspection capabilities of IDS with the blocking capabilities of firewalls. These blocking capabilities, often referred to as active response, allows the detection of a policy violation to be translated in real-time into a policy-based action designed to impede or stop the violation.IPS security solutions are similar to IDS solutions and the two are often used together. These solutions respond to traffic that is identified as suspicious or malicious, blocking requests or ending user sessions.

3.3.3 Event Correlation Systems (ECS)

Event Correlation Systems build on the successes of Intrusion Detection Systems by providing a better mechanism for

aggregating, managing and correlating IDS events, such as are generated through signature detections or policy violations. ECS goes beyond simply pulling together event logs from IDS, however. ECS allows for the aggregation of log data from multiple sources, including firewalls, hosts, applications, and of course IDS. Most ECS solutions serve a dual role as a data warehouse for logs and by providing a data mining interface (manual and automated) to make use of the data stored in the warehouse.

3.4 Endpoint detection and response (EDR)

Endpoint Detection and Response (EDR), is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware. Coined by Gartner's Anton Chuvakin, EDR is defined as a solution that "records and stores endpoint-system-level behaviors, uses various data analytics techniques to detect suspicious system behavior, provides contextual information, blocks malicious activity, and provides remediation suggestions to restore affected systems."

EDR security solutions record the activities and events taking place on endpoints and all workloads, providing security teams with the visibility they need to uncover incidents that would otherwise remain invisible. An EDR solution needs to provide continuous and comprehensive visibility into what is happening on endpoints in real time. An EDR tool should offer advanced threat detection, investigation and response capabilities — including incident data search and investigation alert triage, suspicious activity validation, threat hunting, and malicious activity detection and containment.

3.5 Cloud Security Posture Management (CSPM)

Cloud security posture management (CSPM) automates the identification and remediation of risks across cloud infrastructures, including Infrastructure as a Service (IaaS), Software as a Service (Saas), and Platform as a Service (PaaS). CSPM is used for risk visualization and assessment, incident response, compliance monitoring, and DevOps integration, and can uniformly apply best practices for cloud security to hybrid, multi-cloud, and container environments. It is a set of practices and technologies to evaluate your cloud resources' security. These technologies can scan configurations, compare protections to benchmarks, and ensure that security policies are applied uniformly. Often, CSPM solutions provide recommendations or guidelines for remediation that improve security posture.

3.6 Public Key Infrastructure (PKI)

Public key Infrastructure, also PKI, follows the theory and technology of public key cryptography to provide a universal security service platform for e-commerce. The basic principle is as follows: The third-party authority, the Authentication authority (CA), combines the public key held by the user with the identity information (such as the name

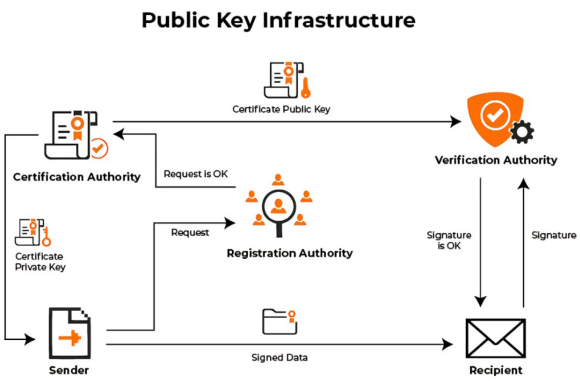

Fig. 9: Public Key Infrastructure (PKI)

and phone number). Before the authentication is combined, the authentication authority (CA) verifies the authenticity of the user's identity. Then the CA signs the certificate bound with the user's public key.

Each user has a pair of public key and private key. The public key is public on the network and is used to encrypt the information when the file is sent. The private key is private, owned only by the user, and is used to decrypt and sign file information. When a message is ready to be sent, the sender encrypts the data to be transmitted using the receiver's public key. After receiving the data, the receiver uses its private key to decrypt it. In this way, users can communicate securely on the PKI service platform.

Based on the identity authentication technology of PKI, digital signature is not replicable, so data integrity and confidentiality are protected. The PKI uses digital certificates issued by a third-party trusted authority (CA) and stored in independent devices such as USB keys and IC smart cards. The certificates are not transmitted over the network. The PKI can prove user identity without online query of the digital certificates. PKI provides a mechanism for restoring and revoking digital certificates. If a user's digital certificate is lost or user information is changed, the PKI technology can restore or revoke the digital certificate to prevent the digital certificate from being stolen or misused. The identity authentication technology based on PKI is flexible and expandable.

However, some researchers point out that PKI is complex and difficult to implement in reality. "Its key deficiencies are its inherently hierarchical and authoritarian nature, its unreasonable presumptions about the security of private keys, a range of other technical and implementation defects, confusions about what it is that a certificate actually provides assurance about, and its inherent privacy-invasiveness." [13]

3.7 Virtual Private Networks (VPN)

A Virtual Private Network (VPN) is a private communications network that makes use of public networks, oftentimes for communication between different organizations. A VPN is not inherently secure, though in its most common incar-

nation it does utilize encryption to ensure the confidentiality of data transmitted. The VPN is often seen as a cheaper solution for deploying a private network than private leased-lines [14] [15]. They often serve to protect and ensure the integrity of communications and may also protect the confidentiality of those communications when utilizing encryption.

Aside from the cost factor, VPNs have two main advantages: they may provide overall encryption for communications and they allow the use of protocols that are otherwise difficult to secure. 44 In contrast, Zwickey sites the two main disadvantages of VPNs being the reliance on ”dangerous” public networks and extending the network that is being protected.

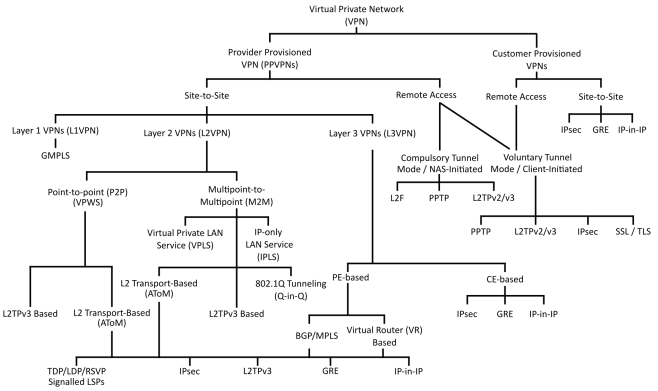

Fig. 10: VPN classification tree based on the topology first, then on the technology used

4 Applications

4.1 Antivirus and Antimalware

Information security can be used to develop Antivirus and Antimalware software for preventing all the digital attacks on the computer and protecting these devices from data breaches, digital attacks, and unauthorized attacks from hackers. It also helps in maintaining network security and firewall systems for all the connected devices on the network.

4.2 Identification and Access Management (IAM)

Identity management and access control is the discipline of managing access to enterprise resources to keep systems and data secure. As a key component of your security architecture, it can help verify your users' identities before granting them the right level of access to workplace systems and information. While people might use the terms identity management, authentication, and access control interchangeably, each of these individually serve as distinct layers for enterprise security processes.

The management has control over which individual can access which sections of the data. Usually, the management regulates who has access to data, networks, and computer systems. Here is where information security comes into the

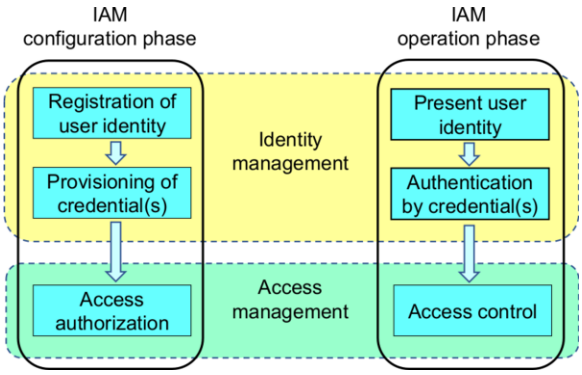

Fig. 11: Identification Management and Access Management

picture by identifying users and executing an access control. Various cyber security applications ensure IAM across an organization. IAM may be implemented in both software and hardware, and it often makes use of role-based access control (RBAC) to limit access to certain system components. Identity and access management systems not only identify, authenticate, and control access for individuals who will be utilizing IT resources but also the hardware and applications employees need to access [16].

4.3 Vulnerability Management

Vulnerability management is a practice meant to reduce inherent risks in an application or system. The idea behind this practice is to discover and patch vulnerabilities before issues are exposed or exploited. The fewer vulnerabilities a component or system has, the more secure the information and resources are.

Vulnerability management practices rely on testing, auditing, and scanning to detect issues. These processes are often automated to ensure that components are evaluated to a specific standard and to ensure vulnerabilities are uncovered as quickly as possible. Another method being used is threat hunting, which involves investigating systems in real-time to identify signs of threats or to locate potential vulnerabilities.

4.4 DDoS Security

DDoS stands for Distributed Denial for Service attack. In this digital attack, the attacker uses multiple numbers of devices to keep the web server engaged in accepting the requests sent by him from the multiple devices. It creates fake website traffic on the server. To deal with this, information security helps to provide a DDoS mitigation service to help cope with it which diverts the traffic to the other cloud-based servers and the situation gets resolved.

4.5 Disaster Recovery

Disaster recovery strategies protect organizations from loss or damage due to unforeseen events. For example, ransomware, natural disasters, or single points of failure.

Disaster recovery strategies typically account for how you can recover information, how you can restore systems, and how you can resume operations. These strategies are often part of a business continuity management (BCM) plan, designed to enable organizations to maintain operations with minimal downtime.

Data recovery enables organizations to continue working in the event of data loss, assaults, or calamities. By regularly data backup and spending money on a system that will enable corporate activities to continue, this application offers models or techniques that may help firms manage with severe data loss. Thus, this application of cybersecurity ensures business continuity.

4.6 Security During Software Development

The software helps detect defects in the software development process and ensures compliance with regulations and standards. Information security tools nip in the works by thoroughly testing, scanning, and analyzing software during development prior to its official release to identify any vulnerabilities, vulnerabilities, or weaknesses that could be exploited by hackers or competitors.

4.7 Health Data Management

Health data management (HDM) facilitates a systematic organization of healthcare data in digital form. Common examples of HDM include: generating electronic medical records (EMR) after doctor visits, scanning handwritten medical notes to store in a digital repository, and electronic health records (EHR).

In addition to organizing medical data, HDR also integrates the information to enable analysis. Information Security plays an considerably important role in health data management. The goal is to make patient care efficient and help derive insights to improve medical outcomes while protecting the security and privacy of healthcare data. Successfully implemented HDM can improve the quality and quantity of health data.

For example, including more relevant variables and ensuring records are up-to-date, validated, and complete for all patients can help improve data quality and increase the quantity. Since more data requires more interpretation, the dataset can grow, and deriving insights can become a complex task for healthcare providers. HDM helps take control of this data.

5 Prospect

5.1 Big Data Security

There are different definitions of the "Big Data" term. The most popular definition is given by describing their three characteristics called "3V": Volume (the data volumes are very large which cannot be processed by traditional methods), Velocity (the data is produced with great velocity and must be captured and processed rapidly) and Variety (variety of data types: structured, semi-structured, and unstructured). Based on data quality, IBM has added a fourth V called: Veracity. However, Oracle has added a fifth V called: Value, highlighting the added value of Big Data [17].

The relation of information security and Big Data is twofold. Information security and privacy are among the most challenging issues of Big Data. At the same time, Big Data analytics promises significant opportunities for solving different information security problems. There are many reports, especially by big companies about Big Data opportunities for information security [18].

Although information security and is critical issues for Big Data, these issues have attracted little attention until now. Some researchers point out that due to big volumes Big Data is unattractive for the attackers for now. But Big Data creates new threats to information security, and ideology of protection adopted for traditional security measures, is no longer adequate for Big Data. Cloud Security Alliance (CSA), a working group which studies Big Data security issues recently prepared a document that lists the tools to protect Big Data systems, including secure computations in distributed programming frameworks, security best practices for non-relational data stores, secure data storage and transactions logs, end-point input validation/filtering, real-time security monitoring, scalable and composable privacy-preserving data mining and analytics, cryptographically enforced data centric security, granular access control, granular audits, data provenance.

As Big Data emerging as a highly promising paradigm for analysis of the large volumes of heterogeneous data, it is changing information security threat landscape and as well as security solutions. However, despite the significant opportunities offered by Big Data for information security, many challenges must be addressed before this potential can be realized fully. Many key challenges in this domain, including detection of advanced persistent attacks, detection of data leakage, incorporation of forensic, fraud and criminal intelligence, and security visualization are only starting to receive attention from the research community [19].

5.2 Artificial Intelligence & InfoSec

Information security and artificial intelligence have a wide variety of interdisciplinary experiences (AI). In information security, AI technologies, such as deep learning, can be implemented to create smart models for implementing malware classification and detection of intrusion and threatening intelligence sensing. In order to combat adversarial machine learning, maintain privacy in machine learning, secure federated learning, etc., AI models need unique cyber security defense and protection technologies.

Traditional security strategies such as signatures are being used to recognize threats. This procedure may function admirably for recently experienced threats, however they are not successful for dangers that have not been found at this point. Signature methods can distinguish about 90 percent of threats. Replacing conventional procedures with Artificial Intelligence can improve the detection rates up

to 95 percent, yet you will get a blast of false positives. The best technique is join both conventional techniques and artificial intelligence. This can bring about 100 percent location rate and limit false positives. Organizations can likewise utilize Artificial Intelligence to improve the danger chasing measure by incorporating behavioural analysis. For instance, you can use AI models to create profiles of each application inside entire network by accessing high volumes of endpoint information [20].

The second decade of the 21st century witnessed the establishment of many information security companies relying on artificial intelligence. Considering the rapid increase in the number of companies providing information security solutions based on artificial intelligence, we can expect that the use of such solutions will become ubiquitous soon. However, It should be noted that artificial intelligence brings not only benefits but also dangers. For example, criminals may create intelligent malware which can automatically scan computer networks for vulnerabilities, create customized tools for cyber-attacks which allow it to penetrate the scanned networks, and find the fastest way to spread to as many computers as possible.

5.3 Cloud Computing

Information security issues exacerbate with growth of Internet as more people and computers join the Web, opening new ways to compromise an ever-increasing amount of information and potential for damages. However, an even bigger challenge to information security has been created with the implementation of Cloud Computing.

In the scenario of Cloud Computing, people are concerned about the privacy of their data because they do not know where their data is being hosted. In a traditional computing center, anything inside the physical firewall boundaries is considered secure. However, a Cloud does not have clear boundaries because of its distributed features.

Customers need assurance that confidential data from their endpoint devices remains protected in a Cloud-based data center. In a computing system inside a data center, various buses connect components. An adversary could physically tap those buses to gain information. This may be possible since an attacker could replace some modules or insert some components in a computer, for example, during the delivery phase. Hence, those buses are not trusted. It is hard for each administrator or privileged personnel from a Cloud Service Provider to get a universal security clearance, especially when a third-party service provider is involved. Cloud Service Providers need to gain their customers' confidence in the claims of data privacy and integrity [21].

Security solutions must make a trade-off between the amount of security and the level of performance cost. The key thesis of this is that security solutions applied to Cloud Computing must span multiple levels and across functions. The goal is spur further discussion on the evolving usage models for Cloud Computing and the increasing security cover these will need to address both the real and perceived issues, thus spurring new research in this area.

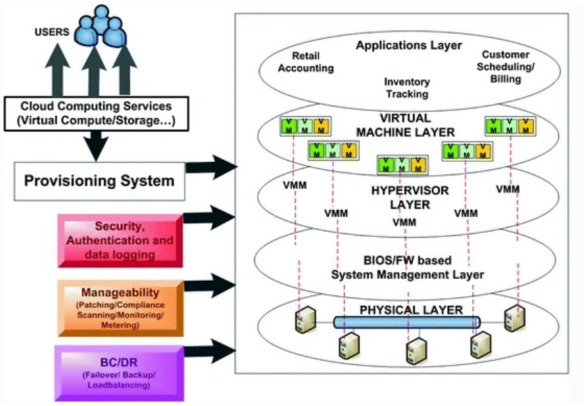

Fig. 12: Security inside a cloud data center

5.4 Blockchain Security

As one of the most hot-debated issue in recent years, blockchain technologies have already changed people's lifestyle in some area due to its great influence on many business or industry. Blockchain has two core features: it is hard to tamper with data, and it is decentralized. Based on these two features, the information recorded by blockchain is more authentic and reliable, which can help solve the problem of people's mutual distrust. According to CIA, here are some advantages that blockchain have to maintain information security:

1. Confidentiality in decentralized systems

The first principle of a strong information security system is confidentiality, which guarantees that sensitive data will not be disclosed to unauthorized parties. This principle is very much in line with a key feature of blockchain: the decentralization of the system. Blockchain is essentially a decentralized system, which means there is no central entry point. If hackers do manage to get into a block of data, they can only steal a small amount of information stored in that block. In addition, because every block in the blockchain is encrypted, it is almost impossible to hack the blockchain system. The confidentiality of organizational information is thus guaranteed.

2. Data integrity and immutability

The second important goal of information security work is integrity. This means protecting data from improper modification or corruption to ensure data consistency. The blockchain system uses encryption to add each new block to the previous one to prevent tampering with the system. In addition, the data stored in the blockchain is transparently visible to anyone with access to the system, allowing errors in the data or gaps in the information to be easily protected. Such systems for recording and storing valuable data can provide companies with what they need to combat data fraud and losses that damage their business.

3. Availability and attacks

The final critical element of a strong, secure information system is timely and reliable access to an organization's data, also known as availability. Cyber attacks typically attempt to limit the availability of information through

domain name servers (DNS) or distributed denial of service (DDoS) attacks. With a decentralized blockchain system, hackers can only target a single vulnerability. The results were far less disastrous; By storing domain information on a distributed ledger on the blockchain, DNS and DDoS attacks will be minimized, and data transfers to iot devices can be securely exchanged across distances, allowing them to communicate and work efficiently.

Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique is also an important topic that we need to concern. As technologies grow and develop, the methods invented to challenge them do the same. Blockchain has a bright future, but organizations must remain vigilant to protect against evolving cybersecurity threats.

6 Conclusion

Beginning with the Caesar cipher around the 17th century, the development of cryptography saw the birth of the field of information security. With the rapid development of computers and the Internet in the mid-20th century, various viruses and network attacks, including Creeper worm, emerged one after another. They seriously threatened information security in different fields, which emphasized the importance of information security protection and promoted the continuous development of information security theory and technology.

Since the CIA triad (confidentiality, integrity and availability) were proposed between the 1970s and 1980s, they have been regarded as three core elements in the field of information security. Various information security technologies keep developing for the purpose of ensuring the confidentiality, integrity and availability of information. With the development of information security, new concepts such as authenticity and non-repudiation have also been put forward by scholars to meet the rapidly changing needs of counting and business.

At present, information security threats are still emerging in an endless stream, with attacks such as APT and DDoS continuing to disrupt network information security day in and day out. At the same time, information security technology is also developing: from the rise of the firewall in the 1990s, to the later PKI, SIEM, etc., more and more counts for information security escort.

Looking forward to the future, computer and information technology has become an integral part of people's life. The deployment of 5G, the advent of the IoT, the current and upcoming cyberphysical autonomous systems, and the envisioned all connected 6G world have all exacerbated the concerns for security and privacy in communication networks. In the next decade and beyond, tens of billions of devices are expected to be collecting and transmitting data over networks. The heterogeneity of these devices in terms of resources and capabilities, e.g., battery power, computational power, The communication and storage "capabilities, renders the approach to date of relying solely on computational approaches for security, e.g., cryptographic solutions, difficult. The emergence of new technologies such as big data, artificial intelligence and blockchain, on the one hand, bring challenges to the field of information security, but on the other hand, also provide new development directions and opportunities. In the cross integration with new technology and new subjects, the subject of information security keeps developing towards a bright future.

References

[1] A. Jones, A. Jones, G. L. Kovacich, and P. G. Luzwick, *Global information warfare: How businesses, governments, and others achieve objectives and attain competitive advantages*. CRC Press, 2002.

[2] S. Samonas and D. Coss, "The cia strikes back: Redefining confidentiality, integrity and availability in security." *Journal of Information System Security*, vol. 10, no. 3, 2014.

[3] A. Firestone, "An information security overview," 2018.

[4] M. A. Elakrat and J. C. Jung, "Development of field programmable gate array–based encryption module to mitigate man-in-the-middle attack for nuclear power plant data communication network," *Nuclear Engineering and Technology*, vol. 50, no. 5, pp. 780–787, 2018.

[5] W. Yu, N. Zhang, X. Fu, and W. Zhao, "Self-disciplinary worms and countermeasures: Modeling and analysis," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 10, pp. 1501–1514, 2009.

[6] N. FitzGerald *et al.*, "Virus-l comp. virus frequently asked questions(faq) v2. 00," *Retrieved March*, vol. 7, p. 2006, 2001.

[7] K. M. M. de Leeuw and J. Bergstra, *The history of information security: a comprehensive handbook*. Elsevier, 2007.

[8] A. R. Miller, "The cryptographic mathematics of enigma," *Cryptologia*, vol. 19, no. 1, pp. 65–80, 1995.

[9] T. J. Misa, "Computer security discourse at rand, sdc, and nsa (1958-1970)," *IEEE Ann. Hist. Comput.*, vol. 38, no. 4, p. 12–25, oct 2016.

[10] N. Boudriga, *Security of mobile communications*. Auerbach Publications, 2009.

[11] E. D. Zwicky, *Building internet firewalls*. O'Reilly Japan, 2002, vol. 1.

[12] P. Innella *et al.*, "The evolution of intrusion detection systems," *Tetrad Digital Integrity*, pp. 1–15, 2001.

[13] R. Clarke, "Conventional public key infrastructure: An artefact ill-fitted to the needs of the information society," in *Proceedings of European Conference on Information Systems (ECIS)*. Citeseer, 2001.

[14] E. D. Zwicky, *Building internet firewalls*. O'Reilly Japan, 2002, vol. 1.

[15] R. Moskowitz, "What is a virtual private network?" 2004.

[16] "Across: A generic framework for attribute-based access control with distributed policies for virtual organizations," *Future Generation Computer Systems*, vol. 78, pp. 1–17, 2018.

[17] A. Baaziz and L. Quoniam, "How to use big data technologies to optimize operations in upstream petroleum industry," *Baaziz, A., & Quoniam, L.(2013). How to use Big Data technologies to optimize operations in Upstream Petroleum Industry. International Journal of Innovation-IJI*, vol. 1, no. 1, pp. 19–25, 2015.

[18] A. A. Cardenas, P. K. Manadhata, and S. P. Rajan, *IEEE Security & Privacy*, vol. 11, no. 6, pp. 74–76, 2013.

[19] R. Alguliyev and Y. Imamverdiyev, "Big data: Big promises for information security," in *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, 2014, pp. 1–4.

[20] V. Vedantam, "Artificial intelligence in information and cyber security," 01 2021.

[21] N. K. Sehgal and P. C. P. Bhatt, *Cloud Computing and Information Security*. Cham: Springer International Publishing, 2018, pp. 93–113.