Master of Science in Internetworking

MINT 709

Capstone Project

On

Analysis of Cybersecurity for The Enterprise

By Shriya Bhat

Under the supervision of

Dr. Mike MacGregor

ACKNOWLEDGMENT

First of all, I would like to thank my supervisor, Dr. Mike MacGregor, for his support and advice throughout the project's progress. Also, his guidance, encouragement and many one-to-one discussions helped me get on the right track towards completing this report. I am also thankful to him for accepting this study and providing valuable suggestions.

I would also like to thank my family for their moral and financial support during my study at the University of Alberta.

Table of Contents

List of Figures

Abstract

Cybersecurity is the process or state of protecting programs, networks, and systems from any cyber-attack. These cyber-attacks are usually aimed at changing, accessing, or destroying sensitive information, extorting money from users, or interrupting normal business processes. In an enterprise, people, processes, and technology must complement one another to create an effective defence from cyber-attacks. All the persons must understand and comply with basic data security principles like choosing strong passwords, being wary of attachments in email, and backing up data. Processes can guide individuals in identifying attacks, protecting systems, detecting and responding to threats, and dealing with attempted and successful cyber-attacks. Technology is essential to give organizations and individuals the computer security tools needed to protect themselves from cyber-attacks. Standard technologies used to protect these entities include next-generation firewalls, DNS filtering, malware protection, antivirus software, and email security solutions.

In today's world, everyone relies on Business Firms, IT Organizations and Medical Services in every aspect. Therefore, the value to protect the data is increasing tremendously. This exponential growth has led to different vulnerabilities, which has accompanied the development of more effective cybersecurity models and mechanisms. But a robust cybersecurity system does not rely solely on cyber defence technology; it depends on people making smart cyber defence choices, effective security plans before any attack can happen. Therefore, when it comes to cybersecurity, an enterprise should instruct all its employees and stakeholders about the advantages of cybersecurity controls. In this way, the company will have less exposure to cybersecurity attacks in the first place. Moreover

, a company will save money with cyber-related loss and severity of cybersecurity incidents when they offer their employees proper cybersecurity training. Another benefit of training employees is the time saved. When a company has fewer cybersecurity threats, its employees will spend less time tracking down the threat, fixing it, and possibly having to redo any affected work. In addition, proper training develops a more positive company culture concerning cybersecurity. The project's gist is to protect entities like computers, smart devices, routers, networks, and the cloud.

Introduction To Cybersecurity

Cybersecurity is a set of measures, rules, means and mechanisms to protect a computer system from unauthorized access, misuse, or attack. Cybersecurity is associated with three main elements as represented in Figure 1: the Human Factor, Processes, Technologies, and their interactions.[1]

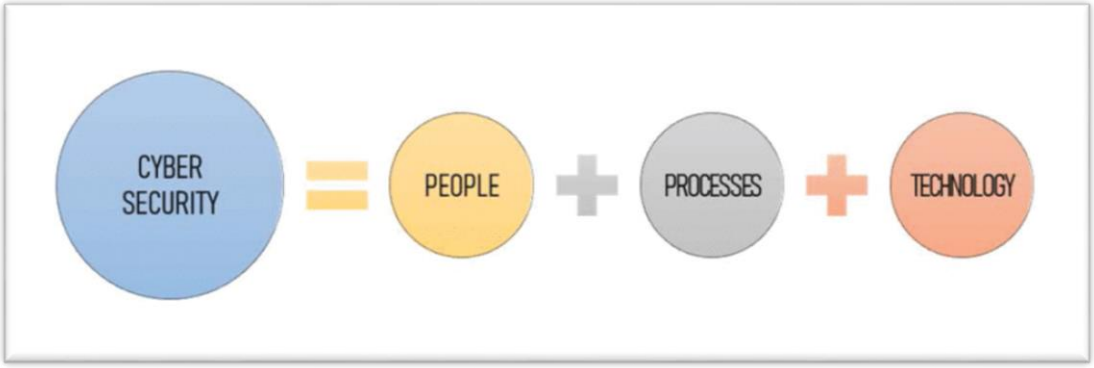

Figure 1:Cybersecurity Attributes [1]

People

The human factor is very critical. It is the primary and weakest link in the security system. It consists of selecting an appropriate password, monitoring suspicious activities, maintaining security awareness. Cybersecurity professionals are entities educated in cybersecurity management, administrators, and rules recipients.

Processes

Processes are steps an organization takes to deal with integrity breaches, information leaks, suppression of service, illegitimate use etc. Processes include:

- User and Role Management
- Plans and services security Testing
- Cybersecurity Audits
- Asset and Risk Management
- Incident response
- Staff Training and Education awareness
- Authorization and authentication

Technology

Technologies are security tools or entities to protect computers, intelligent devices, routers, networks, and the cloud against cyber attacks. Below listed are some standard technologies:

- Intrusion detection and prevention systems
- Malicious code protection
- Network security management
- Active and Offline Backup Systems
- Login systems to Record Activities

CIA Triad

The CIA triad is the three core pillars of cybersecurity: confidentiality, integrity, and availability. The CIA triad is a security model to identify problem areas in a network and provide solutions. Below are these defined:[2]

Confidentiality

All organizations have sensitive information such as client, company, customer, or employee personal identification information. Achieving confidentiality in a network is crucial, allowing only selected users to access specific data. Criminals target organizations with extensive sensitive data as they know that payout (ransom amount) will be high. Attackers often use phishing emails to enter the organization's network and steal passwords or credentials.

An unintentional or intentional data breach can share confidential data with a person who doesn't have access. For example, someone leaving their system unattended, forwarding an email to the wrong sender. However, organizations can take several countermeasures to reduce the likelihood of a data breach and increase confidentiality:

- Implementing administrative policies.
- File and volume encryption.
- Access control list.
- Employee training and awareness.
- Physical hardening such as installing CCTVs.
- Software authentication to control access.

Integrity

The objective of this triad is to provide data assurance, completeness, and accuracy by ensuring that data stays undamaged and unaltered. Data integrity should be essential for both data at flow and rest. Organizations need to ensure that data integrity is implemented by only letting authorized users modify content. Unintentional alterations can result in data loss or network complications.

The cyberwar between criminals and cybersecurity experts is never going to end. Therefore, the companies should take necessary countermeasures like robust authentication methods to identify fake data that looks like actual data.

Availability

Availability ensures that users have prompt and uninterrupted access to networks, systems, and information. It guarantees that data at any time should be accessible to the authorized user without any obstacles such as data breaches or network outages. Denial of services is an unsophisticated attack through which attackers disrupt a company's data availability by flooding a server with multiple requests. This attack degrades services for employees and clients.

Organizations should take countermeasures listed below to strengthen the availability pillar:

- Enterprises should update firewalls and systems regularly.
- Enterprises should monitor endpoints to prevent unwanted traffic on the organization's network.
- Enterprises should reduce redundancies and move to automatic cloud scaling capabilities.

Understanding Myths

Myths are ideas based on errors. Nowadays, companies use advanced tools and technologies to protect their critical assets. But the essential factor is trust, which is lacking in many organizations' cybersecurity initiatives. For example, many cybersecurity professionals or company's business leaders take cybersecurity as a priority only when the risk occurs, and this lack of trust gives rise to myths. There should be transparency about cybersecurity programs for significant benefits among various stakeholders. Students and practitioners need to differentiate between myths and underlying truths because many old assumptions were valid at once but now don't match the reality. Below mentioned are some popular myths in the cybersecurity field:[3]

Myth 1:More layers of defence are always stronger than fewer.

The primary security requirement is to manage and balance the integrity, confidentiality, and availability of assets. A layered defence approach works, as a result, to help the organization reduce the vulnerabilities, but this approach becomes less acceptable when applied to wireless information systems with growing complexities.

Myth 2: If I run the executable on my device, it's secure because I control my system.

Nowadays, a large amount of software is purchased, downloaded, or installed from any site in the system. We use compilers and interpreters to build that software on our system. Still, we do not know whether that tool contains any malicious content (it can download on the system without our detection). As concluded by a great pioneer, Ken Thompon, 'You can't trust code that you did not create'. For example, there was a scandal in 2005 in which Sony BMI's digital rights-management software was installed on the user's device when users played some music CDs on the windows machine. Attackers used that hidden program to spy on users and their listening habits, and neither enterprise could easily uninstall the program. Therefore, it's challenging to determine the security of a complex system where the user is not fully aware of the network's topology, number, and type of connected systems.

Myth 3: Effective security is burdensome

People often feel a system with security measures that are visible, hard to learn, requires significant training is far more effective than systems having security measures that are easy and transparent. But the question is how to ensure that the security mechanism is safer or appears to do so?

Myth 4: Trusted Computing eradicate the need to trust people

People are often confused with the meaning of trust, i.e., if we have no users, the systems would be secure. But the truth is that a computer is a machine that follows instructions to perform computations. So, the actual meaning of 'trust' applied in the context of a computer is how much trustworthy the designer/creator of the computer is. If that person is not reliable, neither is the computer. Therefore, it's equally important to trust the skill and understanding of people who develop the tools. Unfortunately, one popular environment assumption misinterprets the definition of trust. For example, a system is authorized to user 'A' and suppose the user 'A' gives his credential to user 'B'. In that case, the system can't distinguish between user 'A' and user 'B'. The trusted computing systems and the users play a critical role in computer security. By helping people understand these myths, an organization can improve the quality of protection.

Myth 5: If It's encrypted, It's Protected [4]

People often get confused with the theory that if data is encrypted, there are no flaws in the system beyond the fact that secure protocols use cryptography. Still, there are security concerns such as encrypted connection preventing firewalls from utilizing their traffic filtering capabilities.

Need of Cybersecurity

Cybersecurity operations involve protecting confidential information and systems from severe cyber threats. These cyber threats can take many forms. As a result, organizations need to be rapid and robust with cyber security operations and strategies that can be a challenge. In government and enterprise networks, cyber threats take the most innovative and secret form to aim at political, confidential, technological, and military assets of a nation or its people. Some of the common threats are :[5]

Cyber terrorism: Cyber terrorism is a form of attack on computer systems, networks, and telecommunication infrastructures. Terrorist groups innovatively make use of information technology to complete their political agenda.

Cyberwarfare: This involves the nation-state using information technology to undergo damage to another country's networks. In many countries such as the U.S., cyberwar is the fifth domain of war. Well-trained attackers accomplish these attacks to use the benefits of high-standard computer network details to support the nation-state. Instead of closing the target key network, cyberwar attacks can force situations into the network to compromise valuable data, reduce communication and damage infrastructure services.

Cyber espionage uses information technology to gain economic, military, and strategic advantages by using malware techniques. In this, attackers gain access to secret information without permission from its owner or possessor.

Common Pitfalls

Cybersecurity is associated with information security. There are various definitions of cybersecurity, such as securing confidential information with limited sharing and access to information. However, still, the description lacks consent and clarity. Cybersecurity indicates three most important factors, i.e., methods to protect data itself, the transmitted data along with physical or virtual setup and the level of protection obtained. Cybersecurity depends on how individuals take care of data while organizing, managing, and utilizing systems and the internet.

More than 90 percent of systems are vulnerable to cyber attacks, so it is an open ground for cybercriminals. Below are some common reasons mentioned for the cyberattacks:

Internet

Internet is a crucial aspect of our daily life. The easy access and rapid growth of internet services have given rise to cyberization. The development of the internet has impacted various aspects of human life, such as using for studies, surfing social media, watching online videos, doing work or gaming. Also, the screen time has increased during the COVID-19 pandemic, as shown in Figure 2. The graph shows the increase in Canadian screen time during the COVID-19 pandemic. According to the Canadian Internet Use survey (2020), the percentage of Canadian reporting cybersecurity incidents rose from 52% in 2018 to 58% in 2020.[6][7]

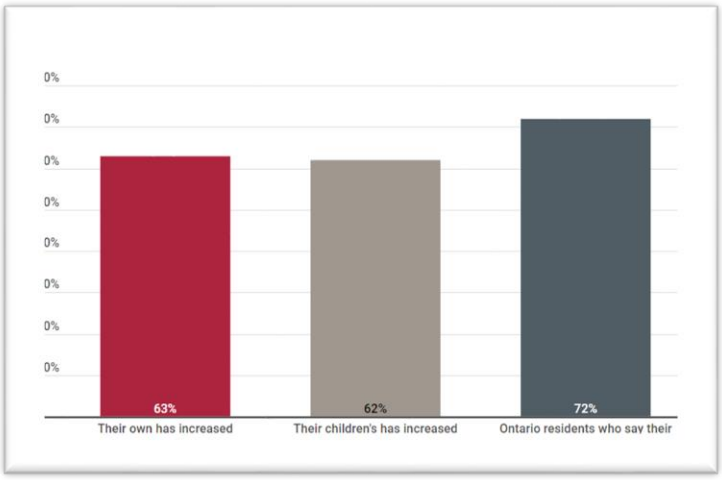

Figure 2: Increase in Canadians' screen time during COVID-19 pandemic [6]

Therefore, it is crucial to look over security concerns and implement strict cybersecurity policies that protect the privacy of information. Cybersecurity is not only confined to protecting computers on the internet, but it is to secure Software, data, news, and hardware from any cyber breach or cyberbullying. People think that cyber threats can only happen to big organizations/institutions, which is a significant interruption. Today more than 60 % of transitions are done online but did a person ever think about, how secure just a click of a button is transmitting his data? The answer to this is cybersecurity. To protect the nation's security, making sure that the internet is safe has become an integral part of development.

Easy to Access

Technology is becoming more complex and heterogeneous, and therefore computer systems are vulnerable to unauthorized access. Attackers use key loggers, advanced voice recorders, retina imagers, implanted logic bombs etc., to fool the system's authorization and bypass firewalls or any security system.

Code Complexity

Nowadays, computer operating systems requires millions of code for designing, which is not 100 percent secure. These gaps gave cybercriminals an advantage to exploit and penetrate computer systems.

Negligence

Cybercriminals often took advantage of human weakness and negligence to exploit a computer system and gain control of confidential data.

Evolution Of Cybersecurity

Traditionally, cyberattacks happened at a single point among Software, hardware, or network level. Primarily, enterprises widely used a perimeter defence strategy to put a wall for protecting all internal resources from destructive external Intrusion. Perimeter defence mechanisms use firewalls, anti-virus software, Intrusion detection/Intrusion prevention systems. Nowadays, IT infrastructure is more hybrid and dynamic. All enterprises are moving from a hardware-based approach to a Software-based policy. Many security solutions work efficiently using traditional perimeter defence mechanisms. In network-based cyberspace, many solutions provide security. Still, conventional security solutions leave an open door for attackers because the perimeter-based tool is not feasible in many cases, such as sensors, services and endpoints managed by cloud providers, intelligent devices owned by employees. The positions of all these systems are in an unattended environment; therefore, a few promising models needs to be advocated by industries:[8]

Software-Defined Perimeter

Transmission Control Protocol/Internet Protocol (TCP/IP) is a fundamental means of communication, including public and private networks. TCP/IP uses IPsec security control to protect data flow between network devices and hosts by authenticating and encrypting data packets from end to end. IPsec supports data integrity and confidentiality through encryption, but TCP/IP-based solutions allow devices to connect first and then authenticate. In this case, attackers get an excellent chance to enter the network channel and disrupt the transmission process before the authentication occurs. The solution to this problem is a Software-defined perimeter, proposed by Cloud Security Alliance(CSA), based on the idea to authenticate first and then connect. It reduces cyberthreat by providing a basic level of securities, i.e., zero availability and zero visibility. Figure 3 shows a clear difference between TCP/IP(traditional approach) and SDP (advanced security model).

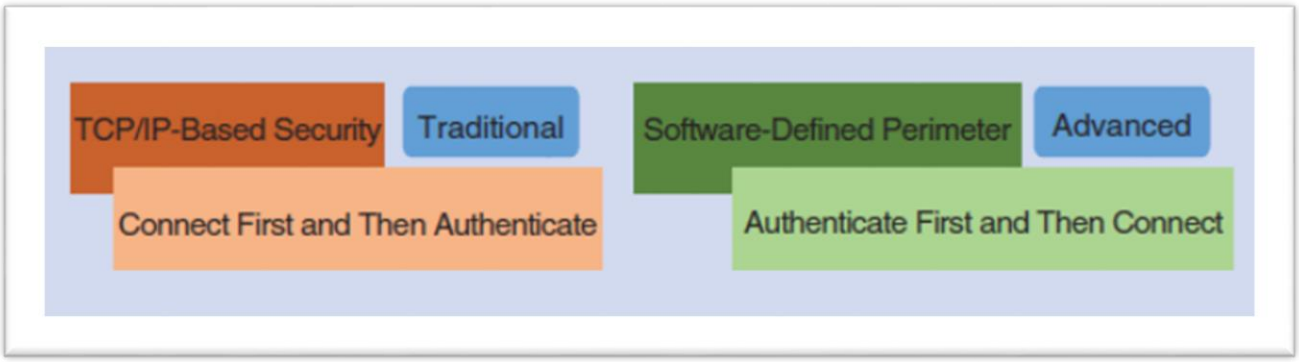

Figure 3: Traditional and Software-Defined Perimeter Security [8]

Nowadays, industries are changing from a static nature to dynamic nature, in which users acquire multiple services simultaneously according to their requirements. CSA published the first version of SDP in April 2014. Any malicious requests are dropped at the SDP gateway without reaching the data center in the software-defined perimeter. SDP provides a cryptographic boundary from a source to a cloud data center by enclosing the origin and destination within the perimeter. The architecture of SDP focuses on three elements:

- security model to verify the access first before connecting over a mutual transport layer security (TLS) connection
- a cryptographic technique to assure that the security model is trustworthy
- a security solution to address any network attacks, including DDOS and man-in-the-middle.

Zero-Trust

It is an appropriate advanced approach for managing end-users and devices. It allows no default trust for any devices/applications/packets/users related to the corporate network. Below is an advanced section on Page 87 that defines the zero-trust model in depth.

Deperimeterization

This advanced multilevel approach fits complex computing systems such as Edge computing, Cloud computation, and IoT. It uses a mix of dynamic data-level authentication and encryption to secure data on many levels.

Cybersecurity layers

Cybersecurity is a multiple layered approach technology to ensure global protection. First, it is most important to understand why a layered approach is more secure, as businesses can more clearly detect malicious bodies and protect their data by minimizing attack vectors. It is mainly critical given the status of threats to be unstable. Therefore, a layered approach is a good quality technique for security. In the early days, cybersecurity professionals were familiar with the OSI model (as shown in Figure 4) as a framework for cybersecurity, but cybersecurity in today's world is much more than networking-only. [9]

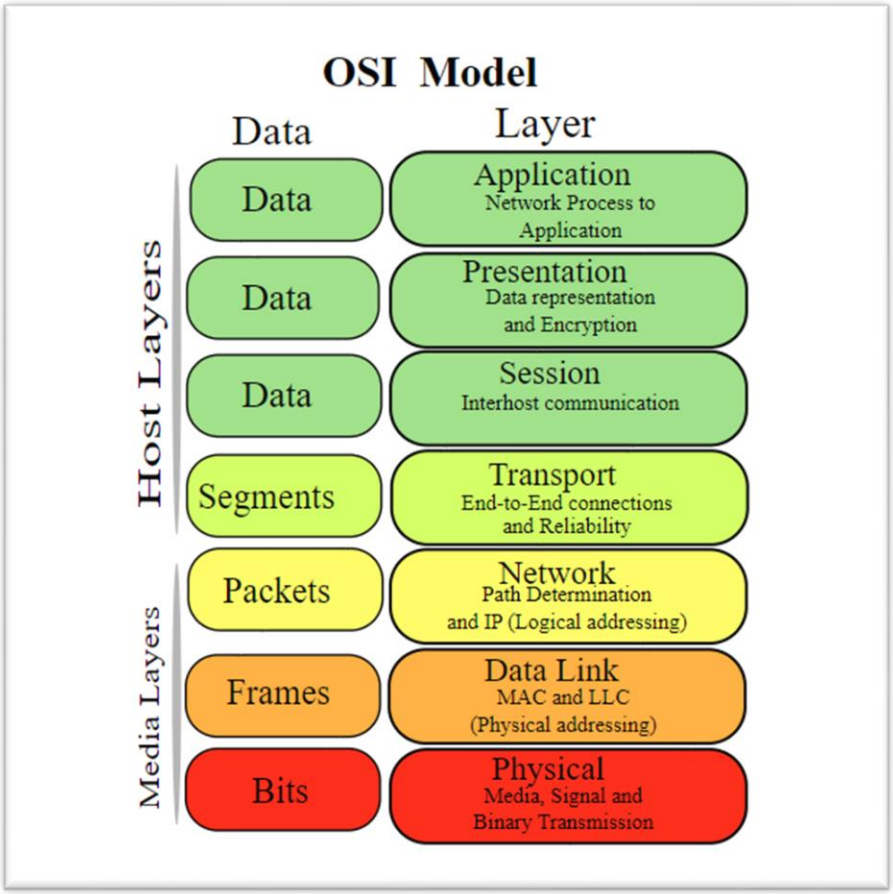

Figure 4: OSI Model [9]

Therefore, a new model was proposed as shown in Figure 5, that goes beyond network domain to perimeter, endpoint, and humans. [9]

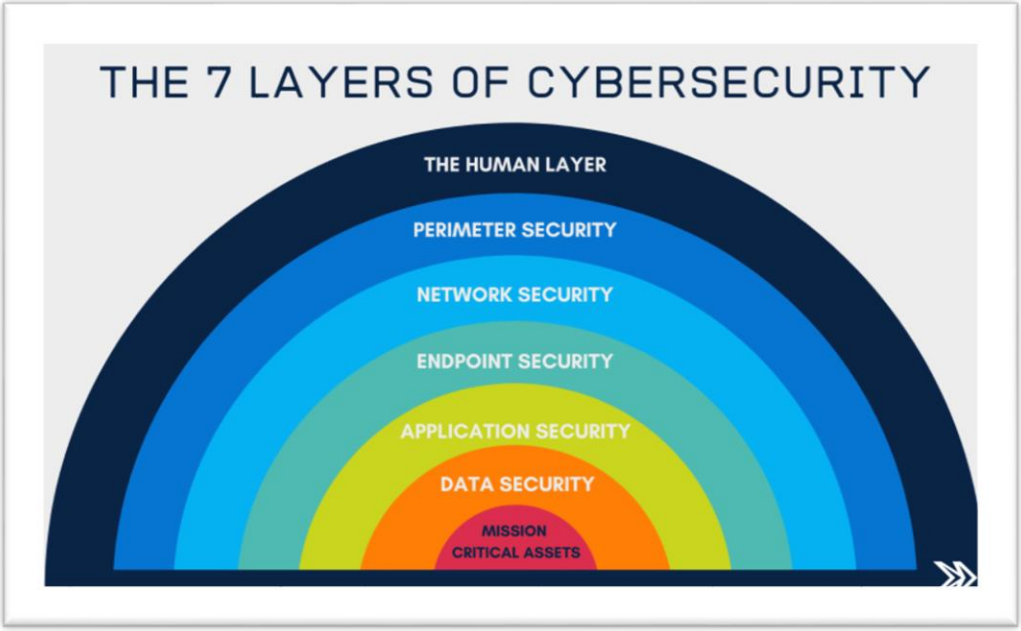

Figure 5:Cybersecurity Layers [9]

Below is a detailed clarification of all the layers:

Mission Critical Assets

These assets are an essential part of an organization and need to be protected at any cost. An example of mission-critical assets in the Healthcare industry is Electronic Media Records; in Financial Sector, it is financial records. However, identifying critical assets is a challenging task, and organizations often lack to determine the intellectual data. The solution to improve an organization's security posture is to understand assets and prioritize them. The Cyber Resilience Review (CRR) classifies the asset into four categories: people, information, technology, and facilities. [10]

Asset management helps an organization plan, identify, document, and manage high-value assets. For example, this whole process is depicted in the Figure 6.

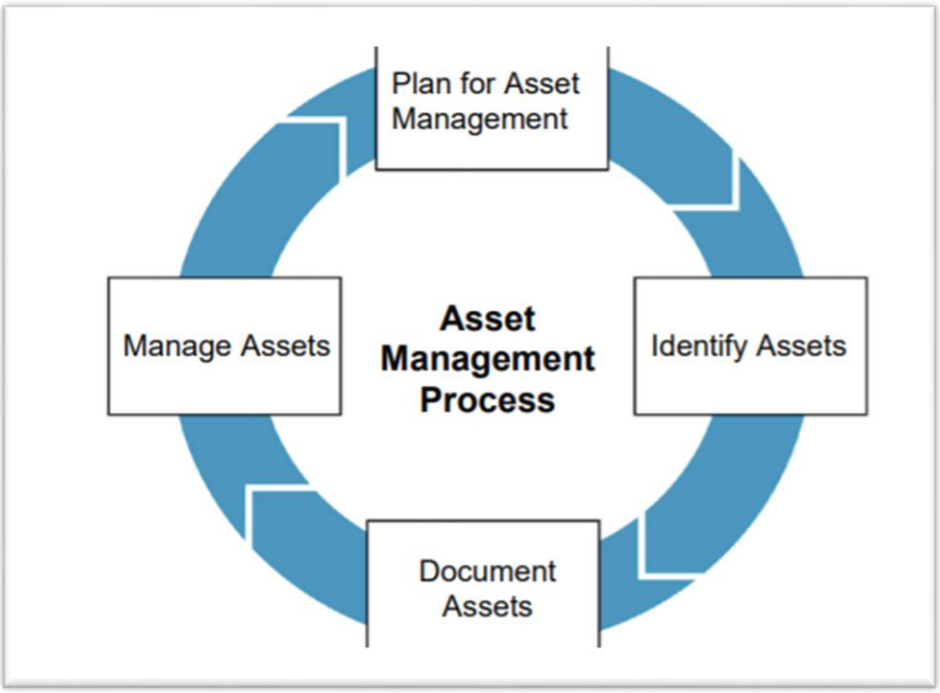

Figure 6: The Asset Management Process [10]

Below is a detailed explanation of how assets are defined:

- *Plan For Asset Management*

Following a plan for asset management makes sure that there is support from higher management, ensuring the plan is fully funded, and there is enough staff to perform. In addition, organizations should focus on essential activities like obtaining permission, identifying the actions required to produce a product, prioritizing those activities, and finally establishing a standard definition of assets within the infrastructure.

- *Identify Assets*

The main focal point of this component is to identify all the external and internal assets of the organization, which includes:

People assets: Employees, Contractors, Visitors, Vendors.

Technology assets: IT systems, Networks, Communications.

Facility assets: Building, Vehicles, Machinery.

- *Document Assets*

Once all the assets are recognized, it is essential to document them to understand their relationship (such as who is responsible for the asset, any changes or update to the asset etc.) to internal/external

organizations. The documented information includes the type of asset, location of the asset, owner of the asset, form of asset (paper or electronic), the asset's value (qualitative or quantitative) etc.

- *Manage Assets*

After documenting all the assets, organizations need to manage assets by selecting tools and methods to determine improvement.

Data Security

Data Security is an essential focus for all businesses to prevent data loss [11]. It contains security controls that must be in place to protect both data transfer and data storage. The most valuable asset to an attacker may be a password, social insurance number, debit card pin. Data is usually stored under three states: at rest, at transit, and in the process. The organization needs to protect the data at each state to maintain Confidentiality, Integrity, and Availability. Data is rest is static data, and its protection is the simplest one because we need to apply encryption or access control mechanisms. One main challenge of protecting data at rest is symmetric key management, in which the same encryption key is used to decrypt and encrypt the data. The solution to this is using asymmetric key encryption. Data at transit involves sending a text message to another user via a wireless connection. Therefore, organizations use asymmetric encryption with HTTPS protocol. The HTTPS protocol uses TLS/SSL (Transport Layer Security/Secure Sockets Layer)while protecting data during transmission.

The last case is a need to protect data while it's in use. An example of data in use is when a user is currently updating, erasing, or accessing any data. Data in use is protected by encryption, and at the same time, enterprises should perform computations on data to decrypt it. An example of such a solution is Homographic encryption, in which analyses are performed on encrypted data without access to the secret key, and then the data is decrypted.

Endpoint Security

Endpoint security ensures that endpoints of users' devices like desktops and laptops are protected whether on the network or in the cloud, depending on the business needs [12]. Endpoint security (also known as Endpoint protection) is an approach to protect the corporate network linked to client devices (such as laptops, mobile phones, ATMs, tablets, Internet-of-things devices). The main goal of endpoint security is to make sure that devices follow a definite level of compliance with standards. Organizations used the Endpoint protection platform (EPP) to protect endpoints from malicious activity and malware attacks. In today's world, with the rise in remote work and

BYOD (Bring your own device) policies, businesses have seen a tremendous increase in the number of endpoints and the type of endpoints. Due to these reasons, endpoint protection platforms have become a must-have for all enterprises in terms of security.

EPP works by scanning files as they enter the corporate network. Modern EPPs also allows storing the data on the cloud, improving the speed and scalability. The EPP provides a centralized console (installed on the network or server) for system administrators or security professionals, allowing them to implement security control for each device remotely. The client software is then initiated on each device using SaaS (Software-as-a-Service) or remotely. Once the endpoints have been set up, client software blocks the use of unsafe applications through encryption. An efficient EPP solution would include EDR functionality to prevent the security attacks from becoming breaches. Organizations use the EDR (Endpoint Detection and Response) platform to maintain endpoint security. EDR allows detecting more advanced persistent threats on endpoints like zero-day attacks, polymorphic attacks, undetectable malware attacks.

EDR platforms monitor endpoints by collecting data through all the sources. The data is then stored in a centralized database and forwarded to the SIEM (Security Information and Event Management) tool for real-time analysis of security alerts. EDR also includes many pre-built popular application components like ServiceNow, Splunk and QRadar.

Despite an organization's best effort to build safe, controlled infrastructures, users will still download and use applications they like. A solution to this problem is endpoint hardening, in which an application is isolated to reduce the attack. Effective application isolation is that:

- Isolates suspicious applications to protect endpoints and networks.
- Protect commonly used applications such as email client's browsers.
- Block exploits by technique rather than by digital signature.
- Block malicious files using threat intelligence.

Application Security

Application security is important because ensuring security at the network level is not enough, but there should be security within the application also. Application security's goal is to implement a secure software development life cycle that improves internal security within applications, that is, accessing and protecting the organization's assets[11]. Below are the different approaches an organization takes while finding security vulnerabilities in the application at different times of the software development lifecycle:

- Before starting to write the code, the architecture and design of an application are reviewed to look for any security problem.
- In the second step, the security engineer reviews the source code of the application to look for any vulnerabilities that will affect the application.
- In the third step, Blackbox security auditing is performed by the organization to look for any flaws. In the Blackbox security audit, the application is tested. There is no need for source code.
- Organizations automate various tools (DAST/SAST) into testing or production environment or CI/CD platforms.
- Organizations could also use various coordinated vulnerability platforms like Bug Bounty Program, in which people can receive compensation for reporting bugs.

Web application Security

Organizations should also take control to secure web applications. Web applications are services that users access through their web browser. Web applications are not on user machines but some remote servers; therefore, web application security is a primary business concern. Enterprise often uses a web application firewall that will block harmful data packets. For example, a web application firewall will monitor, filter and block HTTP traffic to prevent a web application from cyber-attack like SQL injection, Cross-site scripting.

Cloud Application Security:

Application on cloud needs extra care to be authorized. Organizations use the Cloud Access Security Broker (CASB) to protect from vulnerabilities while using cloud services. In addition, CASB helps organizations discover unknown services used by individuals who are not authorized.

Tools for Application Security:

Below defined are some common automated tools to identify vulnerabilities in applications [13]:

- Static Application Security Testing(SAST): SAST is a white-box approach with full access to source code. It can analyze 100% of source code for security flaws even when the application is not in an executable state. This testing tool can give more results and is cheaper to fix a vulnerability at an earlier stage. However, many security warnings can be false-positive and need to verify manually.
- Dynamic Application Security Testing(DAST): DAST is a black-box testing approach in which the tool communicates with a web application using the front-end to identify security

vulnerabilities. DAST tools do not have access to the source code; therefore, they cannot cover the full application.

- Interactive Application Security Testing(IAST): IAST combines the strengths of both SAST and DAST methods providing access to source code, backend connections, HTTP traffic, configuration, and library information.

Network Security

This security aims to prevent unauthorized access (data breaches, intrusions) to a business's network. Network security is essential to keep the data secure and at the same time ensure reliable access and efficient network performance. An enterprise can use the below-defined components for network security [14]:

- *Network Firewalls*

Network firewalls manage outgoing and incoming network traffic using agreed security rules to stop unauthorized access/traffic on private networks connected to the intranet and internet. It relies on all types of firewalls, especially Next-generation firewalls, that shut off malicious attacks like malware and DDOS.

- *Network Segmentation*

Network segmentation separates networks into sub-networks with little connectivity and lateral movement within an organization. For instance, VLANs or IP subnetting can create segments in the network. This method ensures that sensitive data is protected from potential threats as all the hosts are virtually connected. Organizations can also define additional bounds within the network to increase efficiency.

- *Network Access Control*

Network access control is the policy defined in an organization to restrict access of only authorized users or groups to access network applications. One significant advantage of network access control is that the user is authorized based on username/password combination and uses multi-factor authentication. In addition, Identity Access Management (IAM) products can provide strong security controls to protect persons and devices.

- *Remote Access VPN*

Remote Access VPN safeguards an organization's network areas by creating an encrypted tunnel between individual host and organization resources. Hosts have VPN software/web-based client

loaded on their system to maintain the integrity of the organization's and clients assets through data encryption.

- *Cloud Network security*

Organizations are changing from on-prem to cloud-based models, and therefore applications and workloads in today's world are hosted on cloud infrastructure. Hence, it is essential to protect cloud data centers, which requires more significant innovation and flexibility. As a result, enterprises use software-defined wide area network(SD-WAN) solutions that provide network security in public, private, hybrid and cloud-hosted Firewall-as-a-Service deployments.

- *Sandboxing*

Sandboxing is a cybersecurity technique in which files (such as PDF, Microsoft Word, Excel, PowerPoint) are executed in an isolated environment (known as a sandbox) on a host machine/network that impersonates end-user operating environments. Organizations use sandboxing to observe the malicious threat patterns. The primary support of this technique is that it prevents attacks from getting onto the network, avoids system failures, and helps software vulnerabilities spread.

- *Hyperscale Network Security*

Hyperscale is the technique to improve and scale an organization's architecture in case of more demand, which means adding more resources to build a solid and scalable distributed computing network. Organizations use this architecture because it is a very cost-effective approach and reduces the complexities of business operations.

Perimeter Security

This security prevents internal business networks against external networks. Perimeter elements are devices (software or hardware) that connect the organization's internal network to the outside world or vice versa. Below listed are various perimeter security solutions [15]:

- *Perimeter Firewall*

The main task is to inspect packets entering or leaving the network, then accept/block packets based on defined firewall rules. There are many different types of firewall such as packet filtering, Circuit level gateway and proxy server, which performs many networks functions like Network address translation(NAT) and dynamic routing. Nowadays, companies can use a dynamic packet filtering method that stores session information (including IP address port numbers) on the firewall. Companies also use Unified threat Management(UTM) systems which provide more

security(including intrusion detection and application awareness) than packet filtering. However, the best perimeter firewall over UTM and packet filtering nowadays is Next-generation Firewall (NGFW), which examines each packet in depth. NGFW provides optimal network speed, multi-layered protection, SSL termination, application awareness, intrusion detection and prevention, malware scanning and support to NAT and many dynamic routing protocols like OSPF, RIP etc.

- *Perimeter Intrusion Detection and Prevention Systems (IDS/IPS)*

Intrusion Detection/Prevention systems are among the most widely used components for perimeter security. IDS uses statistical techniques to compare the predefined signatures with signatures obtained from the network traffic flow. However, the main disadvantage of IDS is that it can only detect the attack but cannot prevent it. Intrusion Prevention Systems are used to control this situation, which can detect and prevent many predefined web attacks, port scans, incompatible packets, and exploit codes.

- *Demilitarized Zone Security(DMZ)*

The figure 7 shows a DMZ region, defined as an area between the external network and the trusted internal network. The main aim of the DMZ structure is to segregate servers (containing critical information like a database) from the outside web by placing routing devices, FTP servers, mail servers, proxy servers in the DMZ region. By this, the design attacker will not access any elements on the network other than devices under the DMZ region.

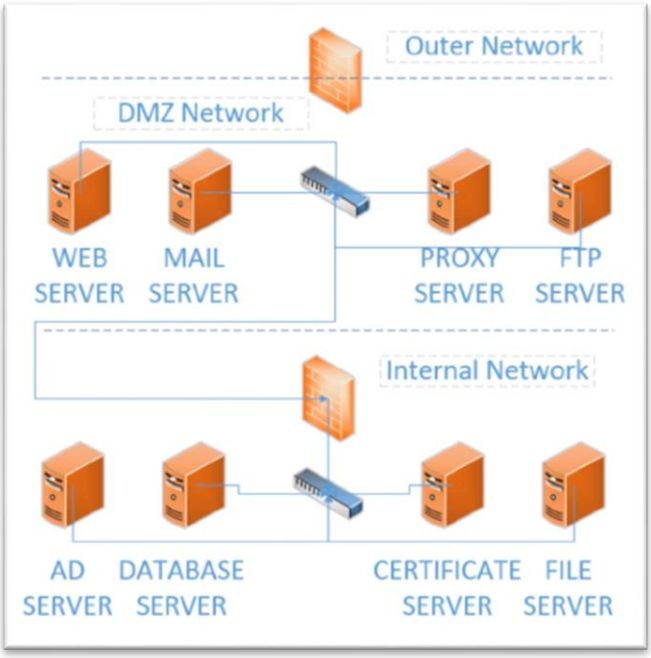

Figure 7: DMZ Network Structure [15]

- *Honeypots*

Honeypot systems are used in perimeter security to understand the methods of attackers. Honeypots are trapped systems with no real value and neither communicate with legitimate systems. Instead, they are placed in the network so that if an attacker interacts with the honeypot, the attacker can be unravelled, and the enterprise can learn the attacker's methods.

- *Data Leakage Prevention Systems (DLP)*

The most considerable panic for an IT organization is when its data is lost or leaked. The main focus of the DLP system is to identify only sensitive data, which is a significant difference from firewalls and IDS/IPS systems that identifies any threat. DLP systems prevent internal data leaks and deter users from causing data loss. For example, if an employee in the IT department is viewing another employee's payroll (belonging to the HR department), the DLP system will create a flag. The figure 8 shows a DLP solution for data in motion. All the traffic leaving the internal network will be transmitted to DLP first for checking the below rules:

- If a sensitive file is transferred over the web, is the file encrypted or not.
- It will check if the file leaving the system is necessary or a violation.
- It will check if third parties on the external network are authorized to see the data in file or not.

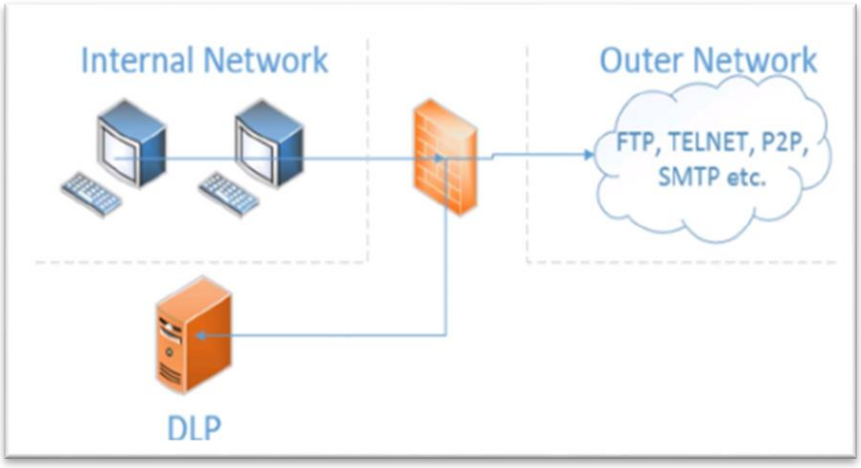

Figure 8: Sensitive content scanning by mirroring on data in motion [15]

Human Layer Security

The human layer is the most infirm link in security. The main aim of this layer is to protect the most critical business assets against phishing simulations, cyber attackers, and malicious users. In an organization, the human layer consists of its people. However, people are dubious and often cause data breaches (either accidentally or maliciously). Nowadays, the disappearance of perimeter security and the growth of cloud technologies and flexible work environments has increased the need for human layer security [16]. There are many causes due to which data breaches by employees can happen:

- Employees often click on a malicious link in a phishing email.
- Unawareness of what information should and shouldn't be shared.
- Sending data to the wrong person.
- Responding to a phishing email.

Unfortunately, not all threats are caused by accidental mistakes. Malicious data breaches occur when individuals feel they can gain from their actions. There are many causes of intentional insider threats mentioned below:

- Employees are taking former organization data to a new job.
- An employee takes data to cybercriminals for receiving a pay-off.
- Employees share essential enterprise data on their systems.
- Employees are leaking data to a competitor.

IMPLEMENTING HUMAN LAYER SECURITY

There are many human layer security technologies like the Zero trust security model, Artificial Intelligence and machine learning that can help in preventing the human layer.

Zero Trust Security Model Approach: This model is based on 'never trust, always verify.' Many organizations have no idea what permissions an employee needs to do their job. Therefore, giving the overly right to do everything on their computer opens the door to installing risky software. For solving this problem, role-based access control is implemented by organizations based on the principle of least privilege and diving the duties depending on job context. Its main aim is to verify if users have appropriate permissions to do their job by continuously evaluating what and how they do it. Organizations also use Contextual machine learning, a combination of techniques and algorithms, to ensure that users email the correct recipients for sharing information. It works by continuously updating user profiles when it becomes available, detecting anomalous recipients, spotting misspelled aliases. Therefore, artificial intelligence and machine learning help organizations determine users behaviours and patterns, reducing the risks of sending emails to the wrong recipients.

Most importantly, organizations should use their employees to mitigate data breaches by giving knowledge of security risks and tools to create a company culture in which there is no fear of retaliatory acts. Moreover, organizations should implement security awareness training that is interactive, engaging, and relevant.

Steps to Build a Layered Cybersecurity Program

- Businesses today have complex environments like remote work cloud computing, which has added new attack vectors. Therefore, the first step towards building an efficient security program is to understand the organization. This includes asking the questions: How many devices? What type of data? What systems?
- The second step is to make sure that what security controls are configured and their effectiveness. Then analyze what decisions need to perform.
- The third step is to ensure that the security program is compliant with all federal regulations and industries.
- The fourth step is to perform repeated testing and analysis of security controls to ensure their effectiveness.
- The final step is to validate that your security program has a backup and disaster recovery and response plan.

Cybersecurity Threats

The cybersecurity threat is a malicious act that aims to damage/steal any computer information asset to acquire unauthorized access to sensitive data (such as Protected Health Information, Education records, personal data). Cybersecurity threats include denial of service attacks, data breaches, computer viruses or attack vendors, either trusted users within an organization or unknown users from remote locations. There are various factors leading to Cyber threats, as shown in the figure 9 [17]:

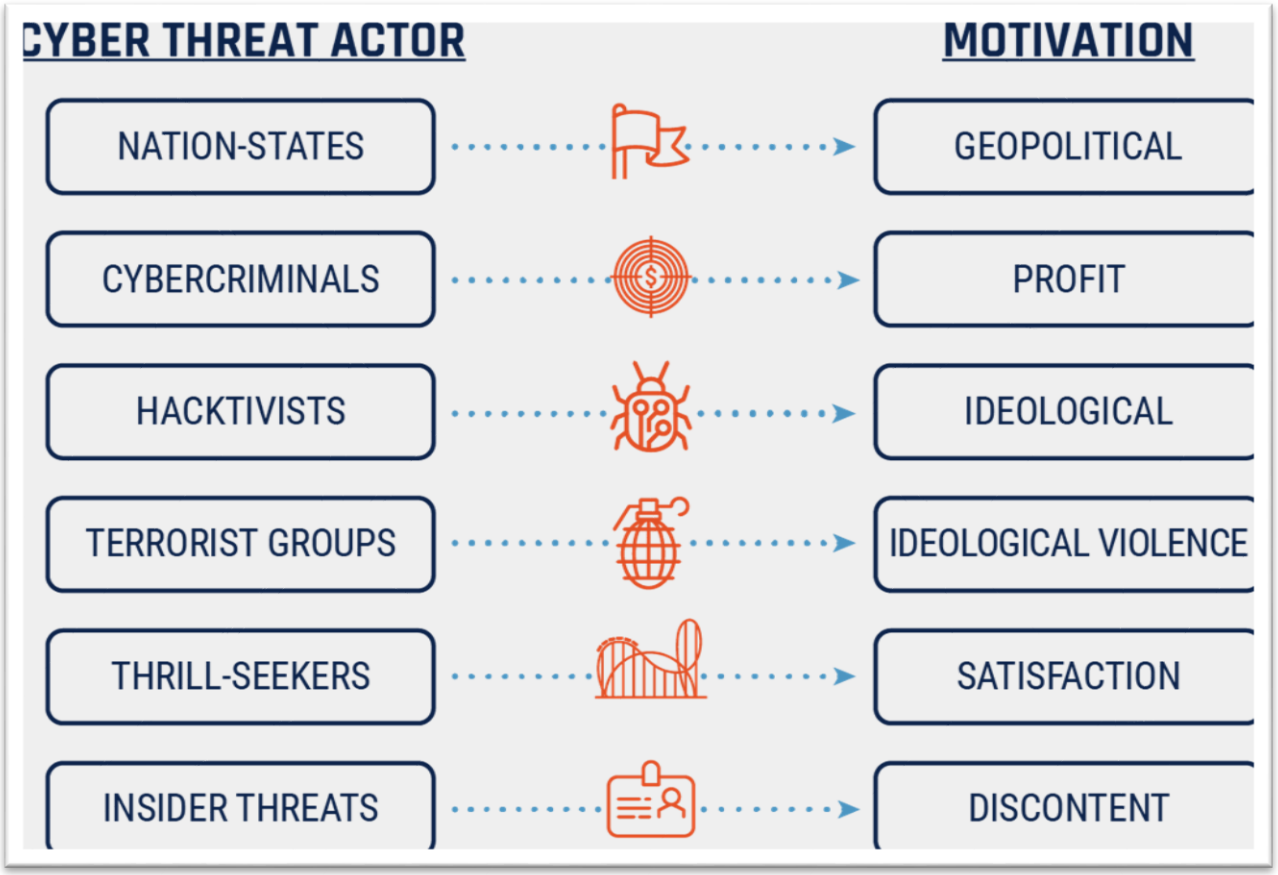

Figure 9: Cyber threat actors [17]

The primary reason for any cyberattack is an unsafe communication protocol and fragile authentication. Tools such as 'Metasploit,' 'SQLNmap,' and 'Meterpreter shell' are used to discover the hidden vulnerabilities by gaining remote access to the infected host once the malware is detected in the system. An attack can be caused by exploiting the system's functionality or vulnerability. Both enterprises and humans are vulnerable to cyberattacks, and the key to better

cybersecurity is to learn and increase the knowledge of cybersecurity threats. Below is a detailed analysis of some common cybersecurity threats:

Malware

Malware, also known as 'malicious software,' can be a code or file that has a malicious intent to infect a system or can virtually perform any behaviour that an attacker wants [19]. For example, if an employee of an enterprise with access to all customer's credit card data tries to sell it to third-party vendors, software bugs like viruses, trojan horses, worms are intentionally added to the computer programs by an attacker. On the other hand, a cybersecurity professional needs to address that sometimes malware can be unintentional due to destructive code, programming errors or flaws and needs to be handled differently. For example, if an employee installed the software using improper parameter settings.

Malware can attack several systems, including Network Devices such as Routers, switches, Modem, Repeaters, End-user systems, Servers, Supervisory control and data acquisition systems. There are many signs that malware has infected your machine, but some common forms are:

- Computer settings being unexpectedly changed.
- Battery draining quickly, leading to downgrading in performance.
- Browser redirects to sites that you did not intend to visit.
- Problems while starting or shutting down your personal computer.
- Frequent pop-ups, warnings by unsolicited groups to buy something to fix them.

Variants of malware as described in Figure 10, caused by Spam, Phishing and Drive-By Downloads:

Trojan Horses[18]: Type of malware hidden as an attachment in any file and cannot make a copy of itself, i.e., it requires user interaction. For example, when the user downloads the file, it gets transferred to the user's device as a legitimate program to steal sensitive information. A famous example can be, when we browse our computer systems and visit different online sites, our screen is filled with different types of advertisements like click here to win an iPhone or download this game. Once a user is tempted to download, it increases of chances of spreading Trojan as we never know which application is chosen by the attacker.

Ransomware: One of the most widespread malware that installs itself into the victim's machine, encrypts file and demand ransom in Bitcoin to return data to the user. 'Wanna Cry' was the most spread malware in 2017.

Virus: This type of malware usually comes as an attachment when we open an email or browse online sites. The attachment has a virus payload, and once the victim downloads the file, the whole system is infected.

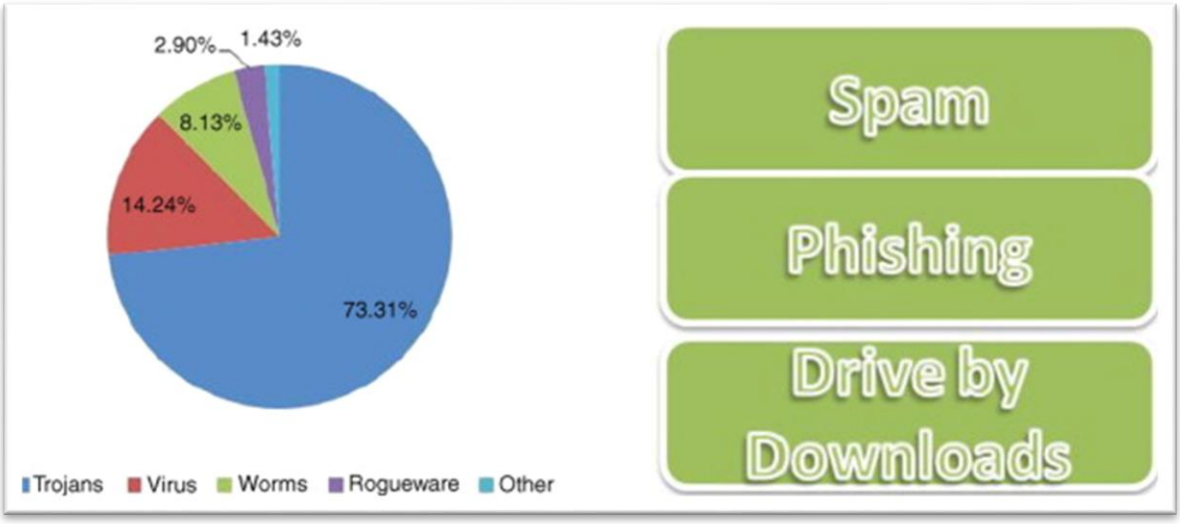

Figure 10: Types of malware and mediums to spread them [19]

Malware attack can happen at any point of network, hardware, or software level. Software trojan, attacks the OS of a computer and leads to stealing or corrupting of sensitive information. Therefore, the first step would be implementing a perimeter defence strategy mechanism to secure a network. It is easier to secure one perimeter than securing many applications, and it is cost-effective. However, the defence strategy is used with access control mechanisms and accountability to authorize and detect any misbehaviours to more defined internal resources.

Below is a table to explain the common attacks and defense strategies.

	Hardware	**Software**	**Network**
Common Attacks	• Hardware trojan (modifying Integrated Circuits)	• Bugs and Flaws in code • Deployment error	• Network Protocol Attacks. • Network sniffing.

	• Outsourcing and buying untrusted hardware to reduce expenses. • Side-Channel Attack (e.g., amount of time and power a process takes)		
Countermeasures	• Tamper Resistant Security Hardware • Trusted Computing Base that will sense the vulnerabilities present in hardware. • Hardware Obfuscation to introduce noises so that physical properties are not compromised.	• Follow coding guidelines and practices.	• Virtual Private Network • Encryption • IDS/IPS • Unified Threat Management Systems • Border Routers • Firewalls

Malware Attacks Analysis by My Doom (worm, 2004)

A mass-mailing worm started in 2004 by flooding the email services, creating the actual doom situation for specific IT companies, thereby slowing the internet services worldwide. It affected Microsoft windows. The figure 11 shows the results from the total virus.[20]

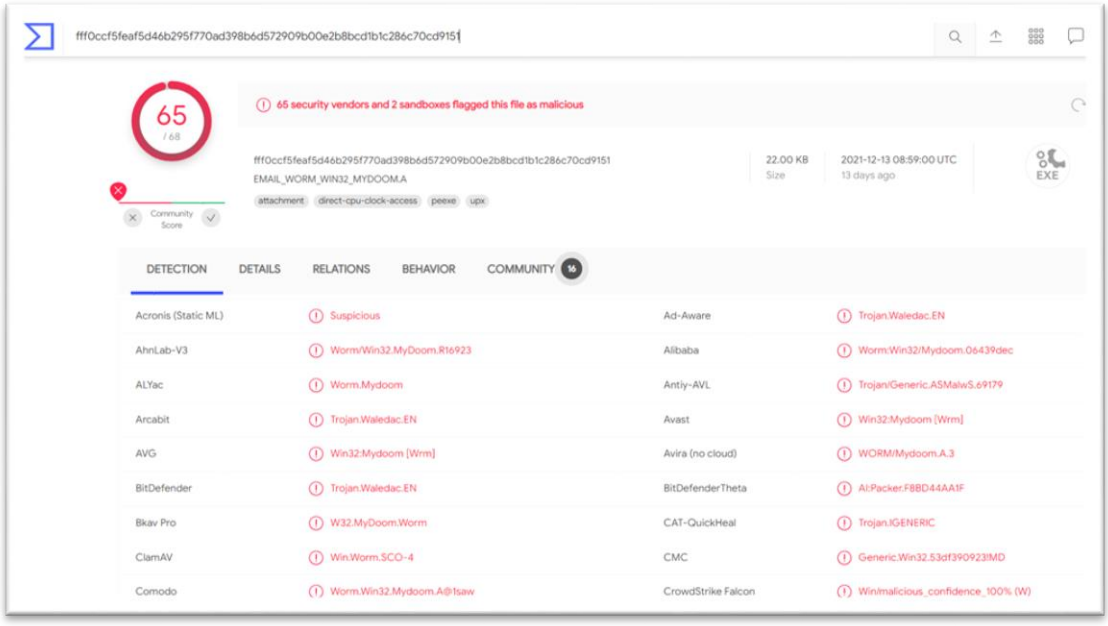

Figure 11: My Doom Analysis [20]

Emotet

Emotet was first detected in 2014 and is known as 'Banking Trojan' because it is a computer program that gets malicious information processed through online banking systems. Since then, Emotet has been following Access-as-a-service (AaaS) or Malware-as-a-service (MaaS) model, which gives Cybercriminals command and control server (C2) functionality which serves as a backdoor for taking complete control of the infected system. The emotet banking trojan has been employed by attackers to deliver other destructive malware payloads like ZeuS, Qbot, IcedID, Qakbot, Trick Bot and Ryuk. The leading cause of emotet is spam emails, also called 'Outlook harvesting.' When a user opens an email and click on any malicious link or download an infectious attachment containing activated macros, malware is automatically downloaded on the system. Once the attacker has access to the network, it tries to use the brute force method to crack the passwords of bank accounts. The Figure 12 represents the emotet detection by country in 2019.[21]

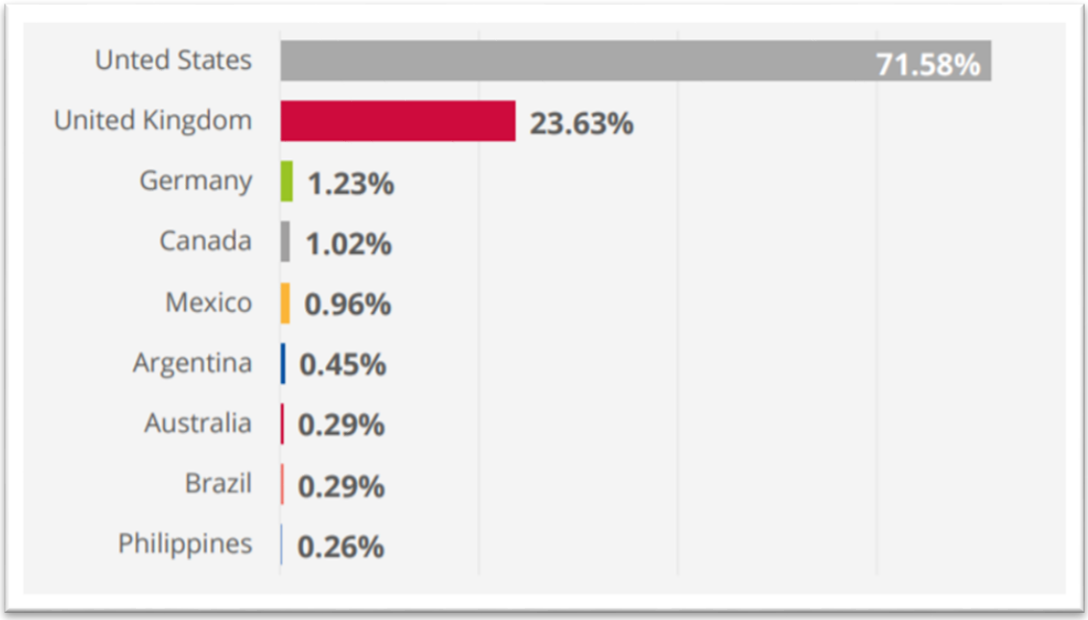

Figure 12: Emotet detection by countries in 2019 [21]

Figure 13 shows a deep technical execution process of emotet:[22]

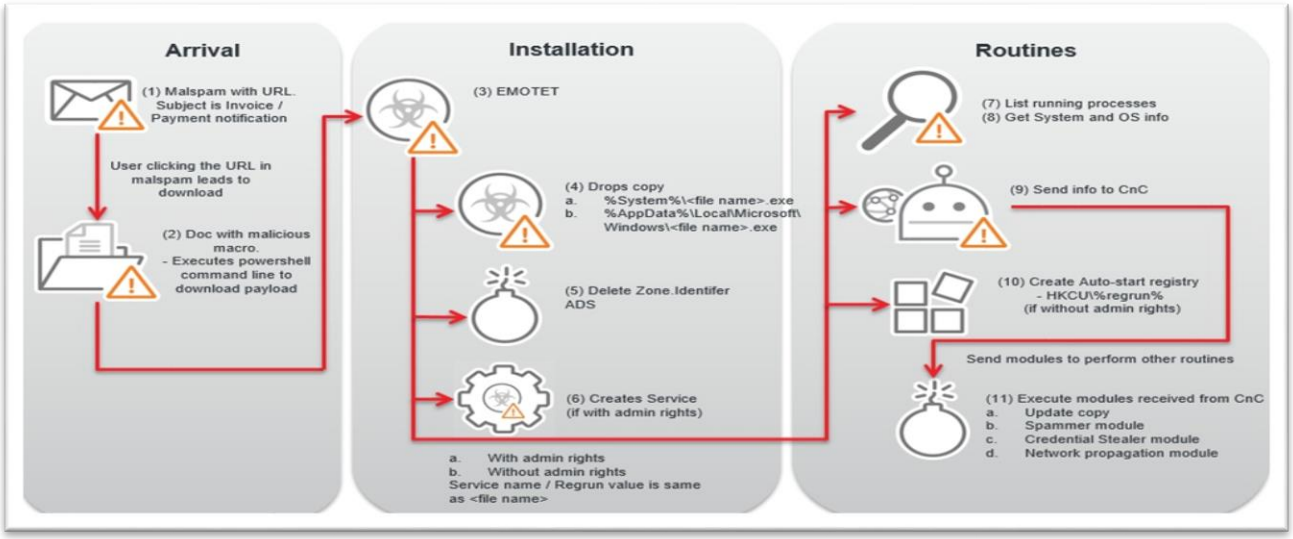

Figure 13: Malware Infection Chain [22]

The distribution of emotet banking trojan is through spam emails and network sniffing. The first step involves the arrival of an email that looks authentic and then luring the user to download a malicious word document attached via a clickable link. Once the document is opened, the user is asked to enable macros that contain VBA (Visual Basic for Applications) code to launch malicious

encoded PowerShell script hidden inside it and download harmful payloads to initiate the infection chain. In the installation phase, emotet copies itself in the AppData subfolders and changes the autorun values. Besides that, the malware sends all system information (system name, location, OS version) and runs processes to and from a server, and in the last step, emotet waits from command and control servers (CnC).

For the defence strategy mechanism, there are some precautions that a person should take to protect against Emotet:[23]

- Be sure to install the security updates for Operating systems (Windows, macOS), application browsers, PDF programs, email clients and office programs to reduce the vulnerabilities.
- Use strong passwords that combine random letters, names, unique characters.
- Do not download any suspicious attachments to enable the macro.
- Block file attachments associated with malware such as .exe and .dll.
- Block suspicious IP addresses at the firewall and apply filters at the email gateway.
- As the C2 server sends messages back to a botnet, it should be blocked for DNS protection.
- Use multi-factor authentication such as confirmation on your smartphone to access your banking portal.
- Verify that cybersecurity controls are in place using the MITRE ATT&CK framework.
- Always have a backup plan in case of any event.

However, emotet case studies from the past represent some common behavioural patterns:

- Multi-layer obfuscation techniques to bypass automated and manual analysis tools.
- Anti-malware technique, i.e., randomization on various places to bypass antimalware solutions.
- Communication through CnC servers using encrypted messages.

Therefore, a multi-level network approach is followed, i.e., an Intrusion response system (IRS) that combines IDS and IPS. When an attacker aims to exploit system vulnerabilities to reach a goal state, a defender attempts to prevent the attacker's progression. Using IRS only action a defender can take is to deploy Iptables, firewall rules blocking either a specific connection between two network hosts or every connection originating from one particular host. By doing this, the IRS will

successfully isolate the machine upon detection of macros being enabled and the communication between CnC servers and bot executables.

Denial Of Service

A Denial of service is a type of cyber attack in which the attacker floods or crashes the victim's machine by sending requests such that the intended machine's resources are fully utilized and unavailable to the user. The flooding of messages forces the target system to be inaccessible and deny the services to authorized users. DOS attack has another type known as Distributed Denial of Service (DDoS). The main difference between DOS and DDoS is that DOS attacks originate from a single attacker while DDoS attack originates from multiple systems such as botnets sitting on the internet. DDoS attacks are more potent than DOS attacks because the attacker first appoints various slave machines and looks for security loopholes by scanning remote machines. Once the vulnerability is known, the device is attacked by malicious code. The infected devices can be used to further appoint agents by sending malicious code to multiple users due to which bots are installed on their systems, and then a botnet network is used to perform the DDoS attack. Usually, in this process attacker hides the identity of the machine by spoofing the source address field. In 2012, Dutch National Research and Educational Network identified Booter. This website offers paid Distributed-Denial-as-a-service that has affected the schools to cancel the exams of hundreds of students. Standard DOS and DDoS attack tools are Shaft, Nemsey, Hulk, Pyloris, Slowloris.

DOS and DDoS attacks can be broadly classified into three categories:

Protocol Attacks: This type of attack is based on the weaknesses in the Internet protocol. Below are the two classic examples of this attack:

- SYN Floods: SYN Floods are the most potent flooding mechanisms. This attack exploits a vulnerability of the TCP three-way handshake. For example: In a TCP/IP 3-way handshake, the server opens a listening port (Port Number: 443) for HTTPS service (for example, https://google.com). When a client (attacker) requests a connection by sending repeated SYN packet to the server on a listening port using a fake IP address, the server (unaware of DOS attack)has to acknowledge all the SYN packets to allocate data structure and will wait for the acknowledgement of its SYN-ACK packet. As the IP address used by the attacker is non-existent, the server waiting for the confirmation will lead all the connections on the memory stack half-open until it times out [26](as seen in Figure 14). During the wait

time, many upcoming packets are flooded by the attacker, leaving the server to crash, and legitimate clients will be denied service. However, on the other hand, the attacker can also use an accurate source IP address and configure the vulnerable machines to compromise the SYN/ACK packet coming from the target IP address.

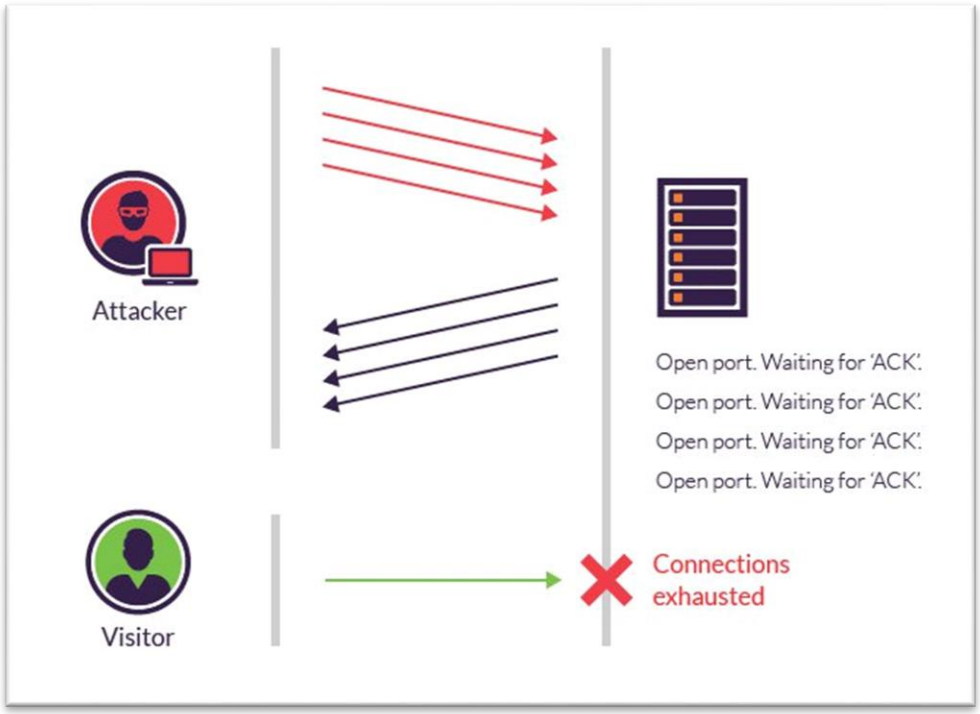

Figure 14: Progression of a SYN flood [26]

- ICMP Floods: The Internet Control Message Protocol uses ICMP packets to diagnose a network. Attackers can execute ICMP flood attacks in two ways. First, the attacker floods the IP broadcast address using the ICMP echo requests packets and the request is forwarded to all the hosts in the network. Secondly, all the network hosts send ICMP echo replies to flood the victim, causing the machine to freeze.

Application Layer Attacks: This type of attack is made by exploiting the vulnerabilities of websites by sending a massive number of queries to the website's search engine, which forces the website to perform memory-intensive CPU operations and leave fewer resources for legitimate users. Below are the examples of this attack:

- HTTP Flood: HTTP Flood is a widespread attack in which an attacker floods the web servers with HTTP requests. As the Internet (WWW) uses HTTP, which runs on a valid TCP

connection over port 80, most firewalls will leave that port open to allow the traffic to pass, making it vulnerable to attack. For example, suppose an attacker targets a website by sending an HTTP request to download a file. In that case, the target machine(victim) will read the file from a hard disk, store into memory, load it into packets and then send it to the botnet(attacker's machine). This repetitive conspicuous activity can take a large resource consumption in input/output devices, CPU, and memory.

- SIP Flood: Today, Voice over IP is popular due to its cheaper rate. As VoIP uses Session Initiation Protocol(SIP) for call setup. The figure 15 explains the VoIP process. If Alice wants to talk to Bob once, Alice has sent an invite for Bob. Alice's SIP proxy server will look for the address of Bob's SIP proxy server and then send an invite packet. Once Bob's SIP proxy receives the invite, it will send the package to Bob's registered address, and his phone will ring. In this type of attack, the attacker will flood Bob's SIP proxy with many SIP proxy invites, and Bob will never be able to get the call from the legitimate user (Alice).[24]

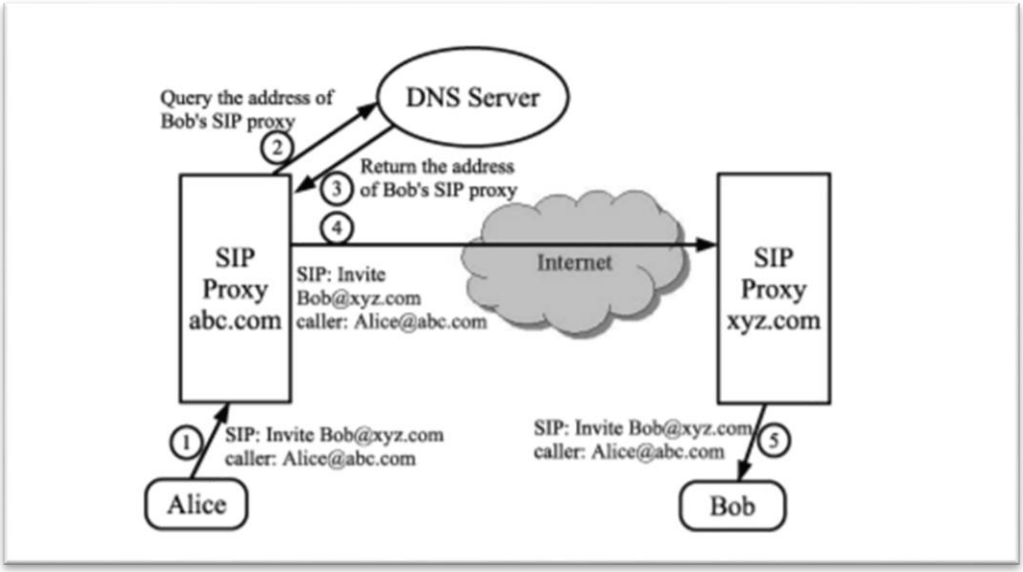

Figure 15: SIP Invite packets [24]

Volume Based Attacks: The main aim of this attack is to saturate the network bandwidth by magnifying the outbound flow of traffic, for example, DNS amplification.

Other common DOS attacks are Ping of Death attacks, Teardrop attack, Bonk Attack, Land Attack.

There are many mechanisms, including authentication and authorization protocols, firewalls, cryptographic algorithms, source identification and packet filtering, IP traceback to reduce the likelihood of DOS/ DDoS attacks. As no one solution fits all the problems, a comprehensive approach is discussed below:[25]

Attack Prevention and pre-emption: The best point to stop a DOS attack is before the attacker reaches its target and causes actual damage. DOS attacks use an IP spoofing mechanism, and the best way is to filter spoofed packets close to the attack sources. It includes Ingress/Egress filtering, allowing the traffic to enter or leave the network only if the source address is within the expected IP range. Other techniques include Router-Based Packet Filtering and source address validity enforcement protocol. The standard limitation of these protocols is that they are not effective if IP spoofing is within the same network of non-spoofed attacks.

Attack Detection and Filtering: It takes place when the DOS attack has occurred. The detection mechanisms can be applied at sources, destination, or intermediate networks, including MULTOPS, SYN detection, batch detection.

Attack Source Identification and reaction: It takes place during or after the DOS attack to filter the attack traffic without disturbing legitimate traffic. IP traceback mechanism is used to identify the attack source.

Man in the Middle

Man in the Middle attack is one of the most popular attacks concerning cybersecurity professionals. It targets the availability, confidentiality, and integrity of the data, i.e., it aims to attack the user's actual data. Man in the middle attack is also known as Session Hijacking, TCP Hijacking, Monkey in the middle attack.[27]

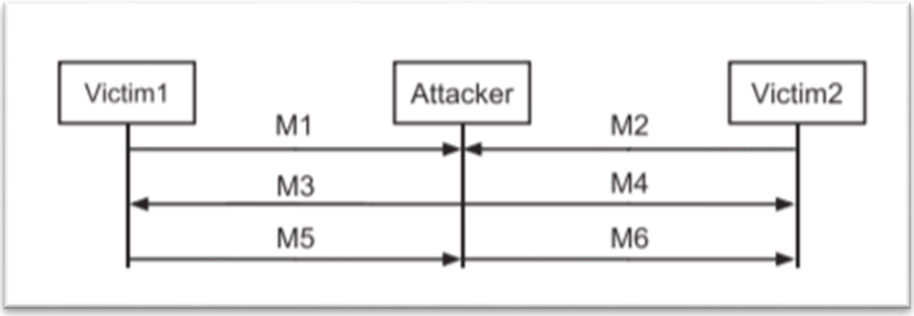

Figure 16: A Survey of Man in The Middle Attacks [27]

Man in the middle attack can be explained using the most common scenario shown in the figure 16. It involves two endpoints (Victim 1, Victim 2) and an attacker. Victims are trying to communicate securely by sending public keys (M1, M2) to each other. An attacker having access to the communication channel is trying to manipulate both Victims by sending public keys M3 to Victim1 and M4 to Victim2. After that, Victim 1 encrypts the message by the attacker's public key (M3) and sends the encrypted message (M5) to Victim2. Attackers obstruct M5 and decrypt the message using the known private key. Then, the attacker encrypts the plain text with the Victim2 public key and sends the message M6 to Victim2. Therefore, the attacker has convinced both the victims to use the secure channel, but in reality, the attacker has access to all the encrypted messages.

MITM attacks can be broadly classified under categories:

Spoofing Based MITM: In this type of attack, the attacker impedes the communication between two hosts by spoofing the attack and taking control of the data. In contrast, the targeted hosts are unaware of the middleman's existence. There are several types of spoofing attack, which includes ARP spoofing(the attacker spoofs victim's device by modifying the victim's ARP cache table), DNS spoofing(the attacker injects fake DNS entries due to which the victim is redirected to a counterfeit website that matches the actual destination), DHCP spoofing, IP spoofing.

SSL/TLS MITM: The SSL/TLS protocol is implemented to ensure that data integrity is maintained by sending the data to the correct destination having access to legitimate users over secure servers. The SSL/TLS MITM attack forges the X.509 certificate, which defines the format of PKI (Public key Infrastructure), that is used to manage the identity and security of computer networks. There are two common ways in which this attack happens. The first way, if an attacker has an invalid

certificate, the attacker can only succeed if the security professionals ignore the warnings, which is a most common problem today. Another way is if an attacker compromises Certificate Authorities (CA) to issue a valid certificate for the targeted web server.

BGP MITM: Also known as BGP Hijacking, the attacker manipulates the traffic to go through the attacker's autonomous system (AS). As a result, the traffic for valid target addresses will never reach the destination.

False Base Station based MITM: In this type of attack, the attacker uses a fake base transceiver station(BTS) to manipulate victim traffic. Using fake BTS, the attacker can inundate a real BTS and force the targeted victims to connect to a fake one.

Prevention mechanism for ARP spoofing against MITM attack:

Enhanced ARP solution(EMR-ARP) is proposed to prevent against Man a middle attack. The whole process is explained in Figure 17. In the EMR-ARP cache (long-term table), the IP address and MAC address are reserved for a long time. However, the ARP cache is, known as the short-term table, reserves the IP and MAC address of all the live machines in the subnet. Three fields, IP, MAC address and Timer, are allocated to each IP address in the long-term table, and the default time is set to 60 minutes. Before the Timer expires, EMR-ARP sends an ARP request to MAC_a to check whether MAC_a is alive and still using IP_a. At random intervals of 100 ms, 10 ARP requests are sent to MAC_a through unicasting to check if the mapping is registered or not. If the mapping is not registered(no ARP reply), the corresponding entry for IP_a, MAC_a, is dropped from the long-term cache.[28]

```
/* (IP_a, MAC_a): the sender protocol (IP) and hardware (MAC)
                  addresses of the received ARP request or reply packet */

if(IP_a is registered in the short-term cache) { --- (A)
  no action; /* in case of conflict, preserve existing mapping.*/
}
else if((IP_a, MAC_a) is registered in the long-term table) {
  register (IP_a, MAC_a) in the short-term cache;
  set the long-term table timer to 60 minutes;
}
else if(IP_a is in the long-term table, but the registered MAC is not MAC_a) { --- (B)
  /* conflict on IP and MAC mapping */
  send 10 ARP requests to existing MAC through unicasting
    at random intervals with an average of 10 msec;
  if(at least one ARP reply arrives)
    retain the existing (IP, MAC) mapping and drop the new one;
  else
    accept the new mapping;
  The accepted mapping is registered in the short-term cache, too.
}
else{ /*i.e. IP_a is not in short-term/long-term tables */ --- (C)
  send voting requests for IP_a;
  if(no response)
    the mapping (IP_a, MAC_a) is registered in both tables;
  else if(there exists a MAC that polls over 50% of votes for IP_a)
    that mapping is registered in both tables;
}
```

Figure 17: short-term cache and long-term table management policies[28]

The above explanation is for Case A and Case B, in which the MAC address is already known. However, in some cases(Case C), the ARP request is coming from a new IP address of a new machine and added into the LAN, whose short-term cache and long-term cache table are empty. In those cases, enterprises use computational puzzle-based voting.

Below are some other best practices that need to be taken to prevent Man-in the middle attack:

- Use of Virtual Private Network to create a secure environment.
- Use of HTTPS over HTTP through the public, private key exchange.
- Make sure to change the router login credentials.
- Strong WEB/WAP encryption on access points.
- Make sure to keep the software up to date by patch fixing.

- Use multifactor authentication to protect your passwords.

Phishing

According to Gartner's report, in 2007, phishing scams cost $3.2 billion in losses exploiting 3.6 million people in the United States. However, from June to December 2009, the phishing attacks increased to 126,697, twice as the first half-year in 2009. In 2010, APWG(Anti Phishing Working Group) reported a professional Phishing crime organization, 'Avalanche,' responsible for the attack in the latter half of the year 2009.

The most common phishing scam today is a deceptive attack in which people's sensitive information is obtained by leading them to access a malicious web page. Clearly, it can be defined as a seven-step process, as shown in the figure 18. In step 1, the user (targeted victim) receives a malicious payload, often through email. In step2, the user is prompted to open a website that seems legitimate as the actual website but is instead an attack page. During steps 3 and 4, the user is asked to enter the credentials for their accounts. The user is lured and enters the sensitive information, and in step 5, those credentials are transferred to the attacker, who mocks the user in step 6. In step7, the phisher steals all the assets in the victim's account. This operation happens so fast that even the user is unaware of this situation. [29]

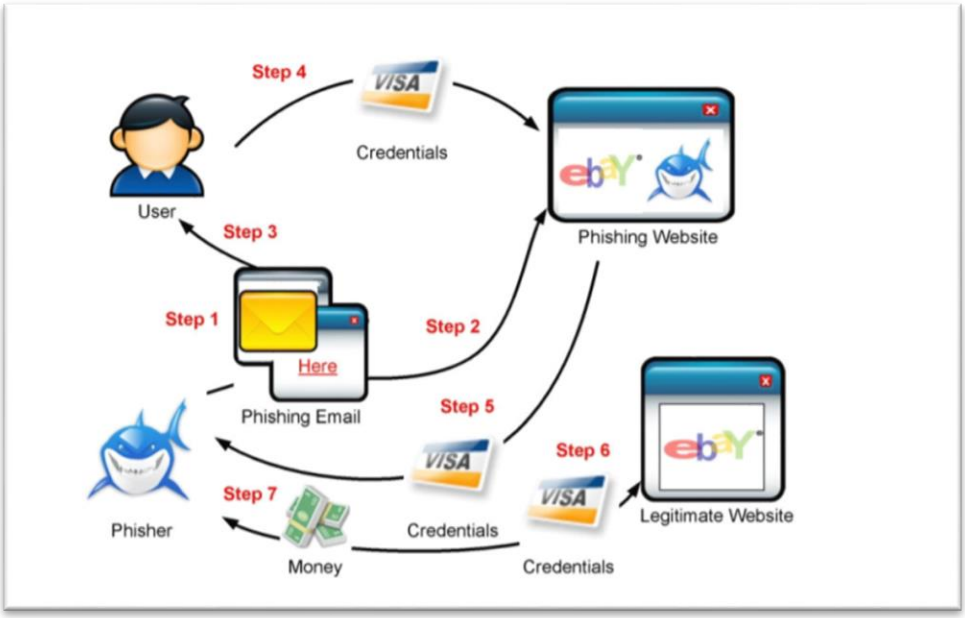

Figure 18: The phishing seven-step process [29]

Existing Anti-Phishing Solutions:

After getting the phishing email to the user, the first protection step is to detect the attack. If the phishing attack is not detected, other mitigation techniques such as offensive defence, corrective, and preventive measures (as shown in Figure 19)cannot be implied. Below explained are some detection techniques:[30]

- *User Training Approach*: User awareness is essential to educate the victims to understand the difference between phishing and legitimate site. Also, users must know the outcome result of their actions. For example, many users ignore the warning failure of the X.509 certificate, which leads to a MITM attack.
- *Software Classification Approach*: In cases where the user base is vast such as Google, PayPal, Amazon, eBay etc., it is difficult and expensive to train a large number of users. Instead, automated software classifiers can be used.
- *URL Blacklisting:* This approach has been practical to some degree as it detects only known phishing URLs. However, this approach does not help detect short-lived phishing webpages as it is time-consuming constructed through human feedback; Netcraft and PhishTank are a few sites to obtain blacklists.
- *Heuristics Rules:* These are applied to the web site's content to check whether it is legitimate or not. Mozilla Firefox, Mozilla Thunderbird, MS Outlook are built with heuristics tests to prevent from phishing attacks. Examples of such applications that apply heuristics rules are PhishGaurd, Phishwish, SpoofGaurd.

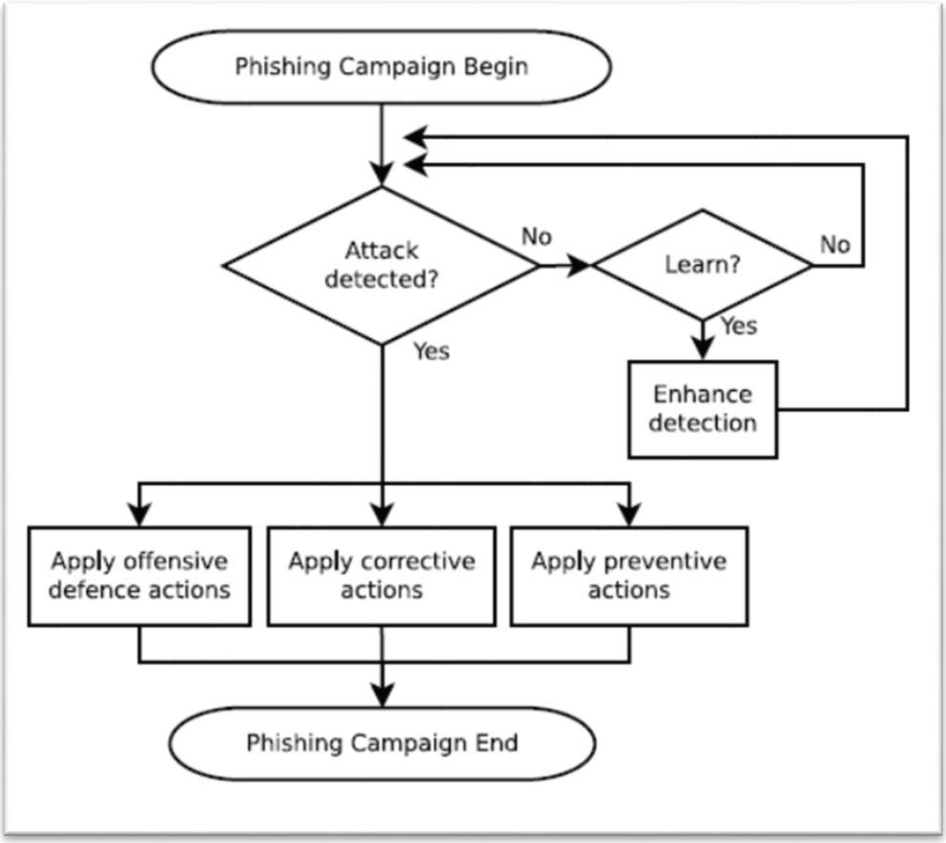

Figure 19: Life-cycle of phishing campaigns from the perspective of anti-phishing techniques [30]

Offensive Defense Actions: This approach makes the phishing attack useless for the attacker by flooding the site with fake credentials so that the attacker finds it difficult to search for the actual credentials. For example, Bogus Biter is a client-side anti-phishing tool that fills fake information in HTML phishing sites. However, if the user base is large, flooding the site with counterfeit credentials can result in a DOS attack leading to the unavailability of the servers.

Corrective Actions: Once the phishing attack has been detected, the aim is to correct it. For example, if the service provider is any website, social networking site or email, the hosting services should be shut down. In addition, Internet Service Providers are responsible for taking down fake websites. According to the PhishLabs report, disassembling down phishing attack sites is helpful. However, it is not a complete and final solution because these sites can still be active for a few days trying to steal customers' credentials before detecting the attack.

Preventive Actions: To prevent future phishing attacks, the users should have knowledge of the attack, so they don't fall victim. Also, Government should suspend all the phishing campaigns started by the attackers.

SQL Injection

SQL Injection is a technique in which security vulnerabilities of any application or website are exploited by injecting wrong SQL queries, i.e., an attacker can inject SQL query from the web form into any SQL database to change the database content or extract dump values like Social Security number, credit card or passwords.

The attacker can compromise the confidentiality, integrity, availability of the application or user by shooting vulnerable SQL statements. According to OWASP(Open Web Application Security Project), SQL injection of code has been categorized as one of the top-10 2010 vulnerabilities exposing the internet. Poor validation of user inputs makes websites vulnerable to SQL injection attacks. There are many defensive mechanisms like IDS/IPS, Firewalls. Still, they are not enough as an attacker performs SQL Injection attacks through regular web ports, which are open in firewalls to allow regular web traffic [31]. SQL is the standard language to access SQL, Oracle, and MySQL servers. Numerous web programming languages such as JAVA, PHP, and ASP .NET support the execution of SQL statements. However, too insecure coding practices, developers often misguide, resulting in vulnerabilities in the SQL code. Below explained are different Types of SQL Injection Attacks:[32],[33],[34]

Tautologies: SQL tokens are passed into conditional query statements (WHERE clause) to be constantly evaluated true in this type of attack. For example, in the below query, passing value 'abc' or '1'='1' to the input parameter password will always become true, and an attacker could get access to the user information.

"Select * from admin_table where username='xyz' and password='abc' OR '1'='1'"

Illegal/Logical Incorrect Queries: Some debug information shows when a SQL query is rejected. The attacker finds this data helpful and uses this debug information to find vulnerable parameters in the application.

Union queries: Attackers use the keyword UNION to join a safe query with an injected query to get information from the database.

Piggy-Backed Queries: In this type of attack, intruders add the illegitimate query after the semicolon (;). By doing this, the database receives and executes multiple queries. For example, in the below query, the database accepts both the queries as the first query ends with a semicolon and then drops the table, which is harmful. Therefore, searching for any unique character in this type of attack is not a solution.

```
Select * from employee where name=’Bhat'; drop table employee
```

Stored Procedure: Attackers use built-in stored procedures to be executed after the legitimate query. These stored procedures are written down after the first original query and sometimes force the database to shut down.

Inference: In this type of attack, attackers change the behaviour of the applications or websites concerning the database.

Blind Injection: This type of inference attack is challenging for the attacker as sometimes the developer hides the debug information and gives a web page asking generic information returning the True/False values. However, if there is no input validation, an attacker can still find the vulnerabilities to attack.

Timing Attack: In this type of attack, the attacker uses the response time function (delay, sleep etc.) that takes some time to finish. By observing timing delays, an attacker can gather information from the databases.

Alternate Encodings: In this technique, attackers escape the special characters (identified by developers as flawed characters) by using an alternate encoding such as Unicode, Hexadecimal and ASCII. This technique aims to avoid being identified by prevention mechanisms. It is executed with other attacks.

Prevent SQL Attacks

There is a wide range of detection and prevention techniques. Those can be broadly defined below:

- Enterprises must reduce the debug information, test web applications regularly and limit web application coding authority. Moreover, developers should configure front-end code and backend databases appropriately, i.e., developers should not only test the code manually because manual testing is a tedious process and will take a lot of resources. Instead, there are several automated testing tools like Burp Suite, Nessus etc., that detect the vulnerabilities before they are exploited.
- Organisation should patch their web application regularly to stop the exploit.
- Data type validation is also a critical approach that developers should use; validating whether the input is numeric, or string helps a lot in determining any mismatched information.
- SQL DOM [38] is a framework suggestion by [39] that enables automated data type validation and escaping by creating dynamic SQL queries using its APIs.
- CANDID, a simple approach proposed by [35],[36] and [37], is a tool that modifies web applications written in JAVA by excavating the programmer's intended query structure against any input and then comparing it against the structure of actual query to detect the attack.
- Intrusion Detection System (IDS) algorithm proposed by [40] monitors JAVA-based applications in real-time by detecting queries that do not match the models of typical queries without producing false positive or false negative.

Advanced Persistent Threats (APT)

Introduction

The advanced persistent threat is a name given to a new type of threat in which attackers target organizations to gain access to their resources. The attackers are very progressive as they have enough organized resources to launch sophisticated attacks. There has been an increase in APT attacks over the last few years. APT groups most often target finance, government, or technology sectors in the USA, South Korea, and Canada. For example, in 2009, attackers performed Aurora operation, resulting in a massive loss to Google's intellectual property [41]. Therefore, APT attacks bring challenges in information security. APTs are a well-coordinated group of people that perform continuing attacks on organizations till they gain access to their computer systems/networks/sensitive data. APTs groups are different from hackers as hackers attack any organization for financial gain or just fun. However, APTs have a particular target, and they don't

stop the attempts till they find a way to compromise the confidentiality, integrity, and availability of the system. Attackers use phishing, social engineering, and other available tools to create malware. Moreover, attackers use advanced knowledge to target zero-day exploits and then use multiple attacks to breach the target system.

Life Cycle of Advanced Persistent Threats

The lifecycle of advanced persistent threats is very complex. Below are the steps listed:

Research

In this step, attackers gather publicly available information about the victim, trying to find any weak points. For example, the attackers search victims' social network profiles, organization websites, communication hierarchy, phishing messages. Once this information is identified, attackers move to the next step.

Preparation

Using the information gathered from the first step, attackers start to extract the information about the victim. Attackers also use many tools and methods such as scanning the network ports, creating customized malware, running vulnerable services that exploit the victim's vulnerabilities. In these steps, the APTs group also prepares the whole foundation, i.e., how to control the attack flow. This process includes modifying DNS entries, taking control of command and control servers, creating fake domains and email accounts etc.

Intrusion

In this step, the attacker launches the attack using a phishing email (considering humans are the weakest link in an organization). This email will lure a victim into clicking on a malicious URL. Other methods of launching an attack can be exploiting a zero-day vulnerability or spreading malware using a removable device.

Conquering the Network

If the attacker successfully enters the organization network, they will gain access to administrative privileges using the victim system. After that, they will create remote administration tools to control the system remotely.

Hiding presence

One main objective of this attack is to remain in the organization network for as long as possible. Therefore, APTs need to hide their presence in the system to avoid detection. To hide their presence, APTs modify the event, install rootkits, modify audit log entries, and delete traces of any susceptible files in the system.

Gathering data

While the attackers are exploring the organization network, they search the data of their interest. Then, the data is encrypted to match the legal traffic on the way out from the organization network using the command and control infrastructure.

Maintaining access

The attackers make sure to get the maximum amount of data while hiding their presence. The attacker also makes sure that the command and control infrastructure is working correctly, and if not, he goes back to the first step.

Notable Attacks

Operation Aurora: Operation aurora was a series of multiple hacking attacks in 2009 that targeted Juniper networks, adobe systems, google, rack space etc. The primary origin of the attack was in China, and the attackers exploited several zero-day vulnerabilities in Internet explorer. As a result, of this attack, Google's intellectual property was also stolen. As a consequence of this, Google left the Chinese market.

RSA: In 2011, it was announced that the RSA security key was a victim of the APT attack. The attacker stole the information about RSA SecureID token seeds and caused $66.3 million damage to the organization. Additionally, the attacker exploited a vulnerability in Adobe flash player by luring victims, by sending a phishing email that contained a malicious excel document. The attackers also use the RAT (Remote Server Administration) tools to control and access the organization's servers.

Stuxnet: In 2010, Stuxnet, a worm, infected industrial control systems, mainly in Iran. The worm destroyed Iran's nuclear centrifuges. The worm cultivated through infected USB drives; exploited zero-day vulnerabilities in the Windows operating system and corrupted programmable logic controller software.

Operation Shady RAT: These attacks started in 2006 and continue till today. In this attack, attackers use encrypted HTML to pass commands to RATs. McAfee reported that this attack had targeted more than 70 organizations in the USA.

Detection

Even if the organization has the best security controls, the system can be compromised. However, there are many defence actions an organization can take to discover malicious APTs:

- If a different type of outgoing traffic doesn't match the typical patterns, it could indicate the presence of malware on the network.
- Organizations should look at internet chat relay (IRC) communication because, in many cases, botnets use IRC to pass control messages between command and control servers.
- Organizations should also check the DNS cache because a typical user does not use an IP address when going out on the network. They generally type any link, and the DNS resolver finds the matching IP address for that user and data is stored in the DNS cache. In a case where an established connection has no entry in the DNS cache, it could indicate a malware infection.
- One main key area for organizations to focus on is to monitor the amount of data sent or extracted. Since APTs pull a large amount of data from organizations that usually is encrypted or masked, analyzing outbound data is necessary.

Various tools exist that can automate network monitoring tasks to help detect breaches in network security:

SNORT

It is open-source intrusion detection and prevention tool that analyzes packets, decodes information in packets, finds patterns within the data and alerts the network. It works on three modes: network intrusion detection, packet logger, and sniffer. The network intrusion detection mode analysis traffic according to a predefined set of rules. The packet logger and sniffer mode store or display packets on the network. In Snort, events can be filtered that helps in reducing the false positives.

SPLUNK

It is a tool that helps users analyze the machine generated big data. Splunk is used in various domains such as IoT, operational analysis, security for searching, indexing, analyzing, and reporting. In addition, Splunk collects data from logs, IDS, and firewalls that have otherwise been escaped from rule-based systems.

Defence

Enterprises can take some preventive measures to stop attackers from breaching the system:

- Organizations should block high-risk applications such as encrypted tunnelling applications, proxies and peer-to-peer programs to facilitate data leakage or malware.
- Organizations need to manage endpoint security by installing and enabling the latest security updates, firewalls, and antivirus programs.
- Organizations should control all external storage media devices like USB driver, optical disks to prevent malware from spreading.
- Organizations should implement strict access and usage policies for wireless and wired networks. Enterprises should enforce Two-factor authentication with the lowest necessary permission level.
- Organizations should implement Network access control for granting access to only those devices that satisfy security requirements such as security patches or antivirus protection.

Cybersecurity Frameworks

NIST Cybersecurity Framework

Introduction

Cybersecurity threats gain advantage from the growing complexity and connectivity of critical infrastructure systems, which can jeopardize the nation's security, company's financial results, economy, health, and public safety. In addition, these risks can increase costs and affect revenues. As a result, cyber security can be an essential and more vital part of an organization's general risk management.

The Cybersecurity Act 2014 (CEA) reformed the role of the NIST framework to increase the robustness of complex infrastructure and support the development of cybersecurity risk frameworks [42]. Through CEA, NIST is recognized as a flexible, repetitive, cost-effective and performance-based approach that critical infrastructure owners can use to identify, diagnose and manage cyber risks. Moreover, NIST is a technology-neutral framework that supports technological innovation while referring to existing standards and norms. Below is a common taxonomy that the NIST framework provides for organizations:

1. Organizations should represent their current cybersecurity posture.
2. Organizations should represent their target sale for cybersecurity.
3. Organizations should identify and prioritize opportunities for continuous improvement.
4. Evaluate the development toward the target sale.
5. Proper communication about cybersecurity risks to external and internal stakeholders.

Components of NIST Framework

The main objective of the NIST framework is to strengthen the communication between cybersecurity activities and business drivers. The framework is composed of three parts listed below:

The Framework Core

It provides a set of activities and instructions to attain cybersecurity outcomes that help manage cybersecurity risk. The NIST framework consists of five functions divided into 23 categories; each category is subdivided into overall 108 subcategories. The core consists of four elements, i.e., functions, categories, subcategories, and informative references, as shown in Figure 20:

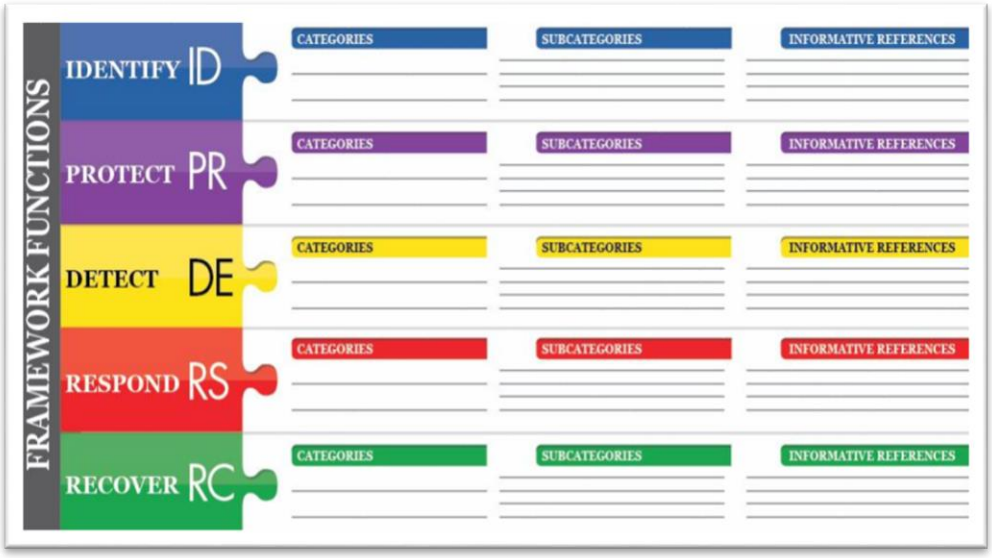

Figure 20: NIST Framework Core Structure [42]

Functions: The functions help an organization to express the management of cybersecurity at the highest level by mitigating risks, managing informative decisions, addressing threats, planning, supporting early response and recovery actions, and making progress by learning from the past. The five framework functions are defined below:

- Identify: The ability of an organization to understand the risk associated with people, systems, assets, and data.
- Protect: Execute appropriate procedures to ensure the safe delivery of critical services.
- Detect: The ability of an organization to determine the occurrence of a cybersecurity event.
- Respond: Implement action regarding detected cybersecurity events.
- Recover: Perform plans to maintain the ability of services impaired during the incident.

Categories: Categories help an organization divide functions into different groups based on the needs of cybersecurity outcomes. Examples of categories are:

- Asset Management (ID.AM)
- Governance (ID.GV)
- Identity Management and Access Control (PR.AC)
- Data Security (PR.DS)
- Detection Process (DE.DP)
- Response Planning (RS.RP)

- Recovery Planning (RC.RP)

Subcategories: Categories divide into subcategories based on technical or management outcomes. Examples of subcategories are:

- Asset Management (ID.AM-4): External information systems are described.
- Governance (ID.GV-4): Governance and risk management processes address cybersecurity risks.
- Identity Management and Access Control (PR.AC-4): Access permissions and authorizations are managed, integrating the principles of least privilege and separation of duties.
- Data Security (PR.DS-5): Protection against data leaks is implemented.
- Detection Process (DE.DP-5): Detection processes are continuously improved.

Informative References: Informative references are guidelines, procedures and standards that demonstrate how to achieve the results associated with each subcategory. For example, for subcategory' ID.AM-4', the security standards are:

- CIS CSC 12
- COBIT 5 APO02.02, APO10.04, DSS01.02
- ISO/IEC 27001:2013 A.11.2.6
- NIST SP 800-53 Rev. 4 AC-20, SA-9

The Framework Implementation Tiers

The organization uses Framework Implementation tiers to describe itself and its stakeholders, how a cybersecurity risk looks, and the level of sophistication of its management approach. The tiers divide into four ranges, and the selection process of Tiers is based on the organization's risk management practices, legal requirements, business objectives, threat level and business constraints.

Partial (Tier 1): Risk is handled in an ad-hoc and reactive manner. Moreover, there is minimal awareness of cybersecurity risk at the enterprise level as the dependents are generally unaware of hazards.

Risk-Informed (Tier 2): In this, the organization is aware of the cybersecurity risks associated with different services but fails to act consistently as the organization-wide approach to managing risks has not been established yet.

Repeatable (Tier 3): The organization-wide approach to managing risks have been established and gets updated as there are changes in business requirements or technology.

Adaptive (Tier 4): An approach to managing risks is based on previous and current lessons learned. Also, there is proactive communication internally and externally to develop and maintain strong relationships.

The framework Profile

A framework profile is an arrangement of functions, categories, and subcategories in a company with an organization's resources. The profile provides a plan for organizations to reduce cybersecurity risks while identifying individual needs. Framework profile compares the 'current profile': which indicates cybersecurity outcomes currently being achieved, and 'Target Profile': which shows the cybersecurity risk management goals needed to succeed. This comparison helps organizations address the gaps necessary to meet cost-effective cybersecurity risk management objectives and define steps for shifting from its current to target profile.

Center for Internet Security (CIS)

Introduction

As users and businesses become more versatile, complexities and dependencies grow, resulting in evolving threats [43]. As defenders, we have access to the best security control tools, training, certification, and classes; all this oversight is becoming 'Fog of More'. It can distract an enterprise from performing a vital action. So, the main question is now that how can an enterprise take the most efficient, defensive, and mature step in a risk management program to address critical solutions?

This question has arisen to 'CIS Critical security Controls' as a solution. The main objective of CIS is to focus on the most valuable and fundamental action that an organization should take and not focus on the 'Fog of More.' The Center for Internet Security (CIS) is a non-profit organization established in October 2000. The mission of this organization (community of individuals and institutions) is:

- Develop and promote best practices to respond to cyber incidents.
- Identify common problems like initial evaluation, implementation blueprints and solve them as a team instead of working alone.
- Identify root causes of the attacks and their defensive actions.
- Share knowledge and tools to solve complex problems.
- Track the growth of threat adversaries and bring regulatory priority to focus on them.

CIS Critical Security Controls Methodology

Actual attacks and successful defences instruct the CIS Critical Security Controls. The knowledge used to reflect on these attacks is combined from every part of the community (individuals, governments, private/public companies, etc.) within many sectors (academia, power, government, IT, Transportation, Finance, etc.) and with every role (threat analysts, policymakers, technology analyst, solution providers, etc.), who have inclined toward each other to create, adopt and support security controls against actual cyber-attacks. Therefore, this ensures that controls are the best defensive and effective measures to detect, prevent, respond and mitigate attacks.

The defensive mechanism identified through these controls reduces the attack by detecting compromised machines, destroying the command and control of the attacker's malicious code, in addition to blocking the initial compromise of systems. The five crucial cyber defence principles reflected in CIS Critical Security Controls are:

Offence informs defence: Take into consideration only those controls that have actual knowledge of real attacks and compromised systems. Using this knowledge will help build the foundation of an effective defence strategy.

Prioritization: Establish a right to first invest in those controls that will help in mitigating the most dangerous threat actors and can be practically implemented in the real-world environment.

Metrics: Exhibit common metrics for IT specialists, security officials, and executives to provide a shared language to implement security measures within an IT organization effectively.

Continuous diagnostics and mitigation: Perform continuous testing and validation of security measures to check the effectiveness.

Automation: Implement automation defences to achieve scalable and reliable compliance to the CIS Security Controls.

CIS Controls

The Centre for Internet Security (CIS) is a set of 20 controls (previously known as SANS Top 20) designed to safeguard organizations from attack vectors. However, the CIS Controls are not a replacement of any existing frameworks, and they map to NIST, PCI DSS and HIPAA. Below defined are the CIS Critical Security Controls:

CSC 1: Inventory of Authorized and Unauthorized Devices

Organizations must keep track of all hardware devices on the network to give access to authorized devices only and quickly identify and disconnect any unauthorized devices from gaining access before they impose any threat.

Why is this control critical?

As new technology evolves day by day, BYOD (Bring your own device: employees can connect their personal devices to office network) is becoming very common in organizations. Unfortunately, employees may have connected BYOD devices in the past to some infected resources, which increases the chance of threat as attackers are continuously looking for devices that come and go off enterprise networks, i.e., systems in which the patches or security updates are out of date. Therefore, enterprises should manage systems in an organization like demonstration systems test/guest systems carefully and, in best cases, should be isolated from other systems to prevent adverse effects.

CSC 2: Inventory of Authorized and Unauthorized Software

Organizations must keep track of all software on the network to install and execute only authorized software and can quickly identify and uninstall any unauthorized software from installation before they impose any threat.

Why is this control critical?

Proper knowledge of what software is being installed in the organization is extremely necessary for data privacy. Attackers use zero-day exploits to find unknown vulnerabilities in vulnerable versions of software that can be operated remotely.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

The organization must implement change control processes to implement security configurations of servers, laptops and workstations. Moreover, companies follow a stringent configuration management process so that attackers cannot exploit vulnerable services and settings.

CSC 4: Continuous Vulnerability Assessment and Remediation

The organization needs to actively gain and assess new information like software updates/ patches and immediately identify and remediate threat actors that could otherwise leave an opportunity for hackers.

CSC 5: Controlled Use of Administrative Privileges

Organizations must automate tools and processes to keep track of how administrative privileges are configured on networks, applications, and computers to prevent unauthorized access.

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

Companies must analyze and manage audit logs that could help investigate and understand security incidents. Without complete event logs, it is challenging for an organization to understand the entire situation and systems that have been compromised in an attack.

CSC 7: Email and Web Browser Protections

The organization must minimize their attack surface because attackers can manipulate human behaviour through forging content on the web browser and email clients.

CSC 8: Malware Defenses

The organization must automate various tools (personal firewalls, antivirus, host-based IPS) at several entry points in the enterprise to monitor workstations and server devices for the execution/installation of malicious code.

CSC 9: Limitation and Control of Network Ports, Protocols, and Services.

The organization should ensure that only essential ports, services and protocols with valid business needs should run on each system. For example, attackers always look for poorly configured DNS servers, web servers, mail servers that increase system vulnerabilities.

CSC 10: Data Recovery Capability

Organizations should use a proven methodology to back up their critical information every week.

CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

Like applications, network infrastructure devices can be exploited and used as a compromised machine to pose as a trusted system by attackers.

CSC 12: Boundary Defense

Attackers often use weaknesses on perimeter network devices to access the enterprise network. Therefore, the organization should implement boundary defence mechanisms such as Intrusion Prevention/ Intrusion detection systems that provide deep visibility over data flow across networks.

CSC 13: Data Protection

The organization should use processes and tools to protect the exfiltration of data to maintain integrity. Data compromise is protected through encryption and data loss prevention techniques.

CSC 14: Controlled Access Based on the Need to Know

Organizations should use processes and tools to track which person, computer, and application is accessing which critical assets based on approved classification.

CSC 15: Wireless Access Control

Organizations must implement processes and tools (vulnerability scanning) to ensure whether the wireless device on the company's network matches the security profile of an authorized user.

CSC 16: Account Monitoring and Control

Organizations must implement critical infrastructure to review the lifecycle of all user accounts. For example, if any former employee or contractor leaves the organization, their credentials should be disabled as soon as possible.

CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps

In cyber defence, the most critical and successful factor is when the user is aware of security gaps. As attackers often lure humans by crafting phishing emails, organizations need to strengthen security by planning and executing training programs.

CSC 18: Application Software Security

Organizations must regularly check if all the applications are running on current/latest versions and if all the patches are up-to-date.

CSC 19: Incident Response and Management

Organizations should implement and develop an incident response plan, which includes proper training, programs, defined roles that help discover an attack more clearly.

CSC 20: Penetration Tests and Red Team Exercises

The final control tests the overall strength of an organization's defence mechanism by carrying out external and internal penetration tests.

HECVAT

Introduction

HECVAT stands for 'Higher Education Community Vendor assessment tool.' It is a questionnaire framework created to assist higher education institutions in determining the vendor risk [44]. The IT environment in campuses is increasing rapidly, and therefore cloud services are always a good option. However, as institutions have a large surface of data (Student's personally identifiable information, research conducted by scholars, financial information) to manage and purchase third-party solutions, attackers continuously target educational institutions for cyber attacks. To help measure the risk and maintain data governance, security professionals from EDUCAUSE's Higher Education Information Security Council (HEISC) developed a tool, 'HECVAT.' According to reports by EDUCAUSE, more than 150 colleges and universities use the HECVAT tool to calculate risk. Below are some main functions of the Higher Education vendor assessment toolkit:

- Ensuring that vendor services are correctly assessed, keeping in mind all the privacy, unique and security concerns essential to higher education.
- Using the HECVAT tool, institutions can reduce costs by implementing a quickly adopted and consistent approach.
- Helps service provides to lower the burden for security assessments.

The HECVAT toolkit is a set of tools that allow higher education institutions to adopt/ implement and maintain consistent security assessments. Toolkit includes:

- HECVAT, Triage: This worksheet is completed by institutions to document technical requirements, data sharing scope and sharing intents with a third party.
- HECVAT, Full: Assessment having over 250 robust questions for most crucial data-sharing arrangements.
- HECVAT, Lite: Lightweight Assessment used for less crucial processes to expedite the process.
- HECVAT, On-Premises: Specific questionnaire for assessing on-premises software and applications.

The HECVAT Full, Lite, and On-Premises assessments have worksheets that should be completed by vendors only who are providing services to institutions. These worksheets aim to deliver complete, robust information assessed to institutions by vendors. In addition, many service providers like Google and Fortinet have shared their complete HECVAT assessments on Community Broker Index, which saves time for institution security professionals to check the posted assessment.

HECVAT Process

Institutions request a third-party solution provider to provide a specific HECVAT version from the toolkit to meet their selection criteria. Then vendors answer all the questions to support their responses like policies, documentation, results of security audits etc. After that, a score is given to all the answers by the institutions. HECVAT is an excellent security assessment filter as it screens out vendors who are serious about keeping your data secure. Vendors who have invested in security audits, their assessments are readily available on CBI, which helps institutions to make a clear perspective on which vendor can meet their particular requirements.

ISO/IEC 27001

Introduction

Organizations are becoming increasingly data-driven due to the rise in business models, technologies, intelligent work practices, and the COVID-19 health crisis. This advancement has expanded the entry points in computer networks and thus their vulnerabilities. Information system

security frameworks and standards have contributed a vital role in securing the data (for example, financial data, customer details, intellectual property and employee records). In particular, to all those standards (ISO 9001 and ISO 14001), ISO/IEC 27001 has become the most acclaimed certification for establishing, implementing, maintaining and continually improving an ISMS (Information Security Management System) applicable to all organizations regardless of type, nature or size. In 2005, ISO (International Organisation for Standardization) and IEC(International Electrotechnical Commission) jointly published this standard and was revised in 2013. As in the previous sections, we have defined another security framework, NIST. So, what is the main difference between NIST and ISO 27001?

As a U.S government agency that promotes NIST, ISO 27001 is an international standard. Moreover, enterprises can jointly use NIST SP 800 series and ISO 27001 to implement security.

How does the standard work?

ISO/IEC 27001 standard demands that service providers include proper risk management, information security and business continuity. The benefits include:

- Organizations should follow an organized method to examine security risks considering all the threats, vulnerabilities, and impacts.
- Organizations should follow a systematic and flexible approach (risk avoidance, risk transfer) to address those risks that are intolerable.
- Organizations should keep track on an ongoing basis to check if security controls meet the organization's security needs. To check if security controls are operating effectively according to the organization is reviewed by the security auditor.

There are a few ways in which enterprises can implement ISO 27001 controls:

Technical Controls: Implemented using software/hardware components. For example, Antivirus software.

Organizational Controls: Implemented by executing and defining rules. For example, Access Control policy, Bring your own device Policy.

Legal Controls: Implemented by enforcing laws and regulations. For example, Non-Disclosure Agreement (NDA), Service Level Agreement (SLA).

Physical Controls: Implemented by using physical devices. For example, CCTV cameras, alarm systems and locks.

Human resource Controls: Implemented by providing awareness training, knowledge, skills, education to people in the organization.

ISO/IEC 27001 Certification

Certification to be certified ISMS system is verified by certification bodies (also known as registration/ assessment bodies or registrars). The ISO/IEC 27001 certification has a three-stage external audit process:[47]

Stage 1: This stage has an informal review to familiarize the organization with auditors and vice versa. For example, checking the Risk treatment plan, Statement of Applicability and security policy.

Stage 2: This stage has a more formal and detailed review in which the auditors test the ISMS systems against the requirements specified in ISO/IEC 27001. After passing this stage, the particular ISMS is ISO/IEC 27001 certified.

Stage 3: This stage includes periodic reassessment audits to confirm that the organization is still in compliance with the standard specified and agreed upon.

Standard Structure

Creating an ISO compliant ISMS is a complex process that includes clauses listed in Figure 21 [45]:

Figure 21: ISO 27001 Compliance Steps [45]

Organizational context: All the external and internal issues affecting an ISMS need to be determined.

Scope: After determining the issues from the first step, the scope of ISMS needs to be documented for the overall management structure.

Leadership: Leadership skills are essential in maintaining the ISMS, for example, Building a security policy in the right direction of the organization.

Planning: A proper plan for the risk management process should be integrated into ISMS. For example, Risk analysis, identifying risks, evaluating risks according to risk criteria, risk treatment (mitigating threats).

Support: An enterprise needs to provide proper support for ISMS. For example, train the staff on how to deal with information by implementing appropriate methods of communication.

Operations: All the processes defined in the previous sections needs to be executed as planned.

Performance evaluation: Organisations need to conduct internal audits to ensure future improvements of ISMS.

Improvement: If there are any issues, immediate steps need to be executed to improve the effectiveness of ISMS.

Controls

There are 114 controls in 14 groups and 35 control categories:[46]

A.5: Information security policies (2 controls): The controls listed in this domain describe how to manage direction and support for information security policies concerning valid laws and regulations.

A.6: Organization of information security (7 controls): The controls classified in this domain focus on executing and operating security controls within an internal organization.

A.7: Human resource security (6 controls): This control is applied before, during, or after employment to help employees and contractors understand their roles and responsibilities. Moreover, it helps understand what will happen if an employee leaves the organization or changes their position.

A.8: Asset management (10 controls): The main objective of this annex is to understand the responsibility of information assets, i.e., rules for ownership of assets, use of assets and return of assets.

A.9: Access control (14 controls): The main aim of this annex is to ensure safeguard control procedure, i.e., employees can view information according to their business needs.

A.10: Cryptography (2 controls): The main objective of this annex is to maintain the confidentiality and integrity of information by ensuring proper and effective cryptographic solutions.

A.11: Physical and environmental security (15 controls): The controls in this annex ensure that enterprises should protect access to all physical areas equipment from unauthorized entry (like attackers).

A.12: Operations security (14 controls): The controls in this section require ways to record incidents and generate evidence, regularly check for vulnerabilities, and take measures to prevent auditory activities from affecting operations.

A.13: Communications security (7 controls): The controls mentioned in this annex show how a network, its services, infrastructure and information are protected.

A.14: System acquisition, development and maintenance (13 controls): The control focuses on ensuring that whenever an organization needs to buy any new information system or needs to upgrade the existing ones, necessary information security controls should be taken into account.

A.15: Supplier relationships (5 controls): The controls defined under this section make sure that activities performed by solution providers, vendors, suppliers and partners should also use security controls to monitor their performance.

A.16: Information security incident management (7 controls): The main objective of this annex is to handle security events following a quick, effective and timely response to address information security incidents, events and weaknesses

A.17: Information security aspects of business continuity management (4 controls): The main objective of this annex is to ensure that business continuity should be intact if any adverse situations (for example, disaster or crisis)occur.

A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls): The main objective of this annex is to prevent violation of legal, statutory or contractual obligations connected to any information security requirements.

Authentication Methods

Authentication plays a crucial role in implementing the confidentiality of the user. For example, whenever we log in to our online banking, we enter our username and credential, but who is authorized in making sure that the credentials are correct. The answer to this question is authenticating the server that stores all the credentials, and at the time of login, it verifies the credentials. If correct, the server authenticates us. Below are some authentication protocols used in environments like wireless or remote [48]:

EAP-MD5(Extensible Authentication Protocol- Message Digest): In this method, the RADIUS (Remote Authentication Dial-In User Service) server regulates authentication using the MD5 algorithms. The operation is performed on the user's name and password by the server, which stores the MD5 hashes of the password. Then, the client sends the hash of its password to the RADIUS server, which compares the received hash and the hash password stored in the database. If the password match, the client is authenticated. However, this authentication method can only verify the client, not the server; therefore, it lacks mutual authentication.

EAP-TLS(Extensible Authentication Protocol-Transport Layer Security): It is the most secure EAP standard developed by Microsoft. This method provides mutual authentication (as shown in Figure 22), which requires installing X.509 certificate on both server and client machine, which causes higher management costs. In this, the client and server exchange X.509 certificate and negotiate a session encryption key which is then passed to the access point by the server to allow the client to access the network.

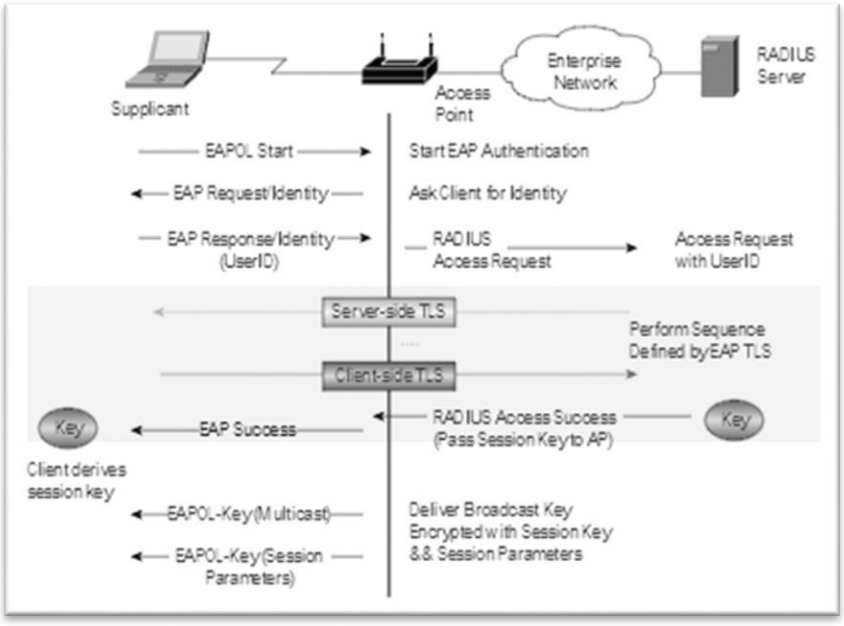

Figure 22: EAP-TLS Authentication [48]

Complete EAP method: This method fully meets the requirement of RFC 4017, as it avoids exponential computation by using secure symmetric encryption and hash functions. It also discards the installation of certificates on both the server and client-side. It uses stored secrets and passwords to verify the user.

Authentication Factors

Below are the various factors affecting authentication as shown in Figure 23:[49]

- Something you know (Knowledge Factor): For example, Credit/Debit PIN, Password, Social security Number.
- Something you have(Ownership Factor): For example, Credit/Debit card, smart card, ID card, Hardware/software token(Fobs is a kind of hardware token embedded with a program to give access to buildings etc.).
- Something you are (inherence Factor): For example, Handprint, Fingerprint, IRIS scan, Face Scan.

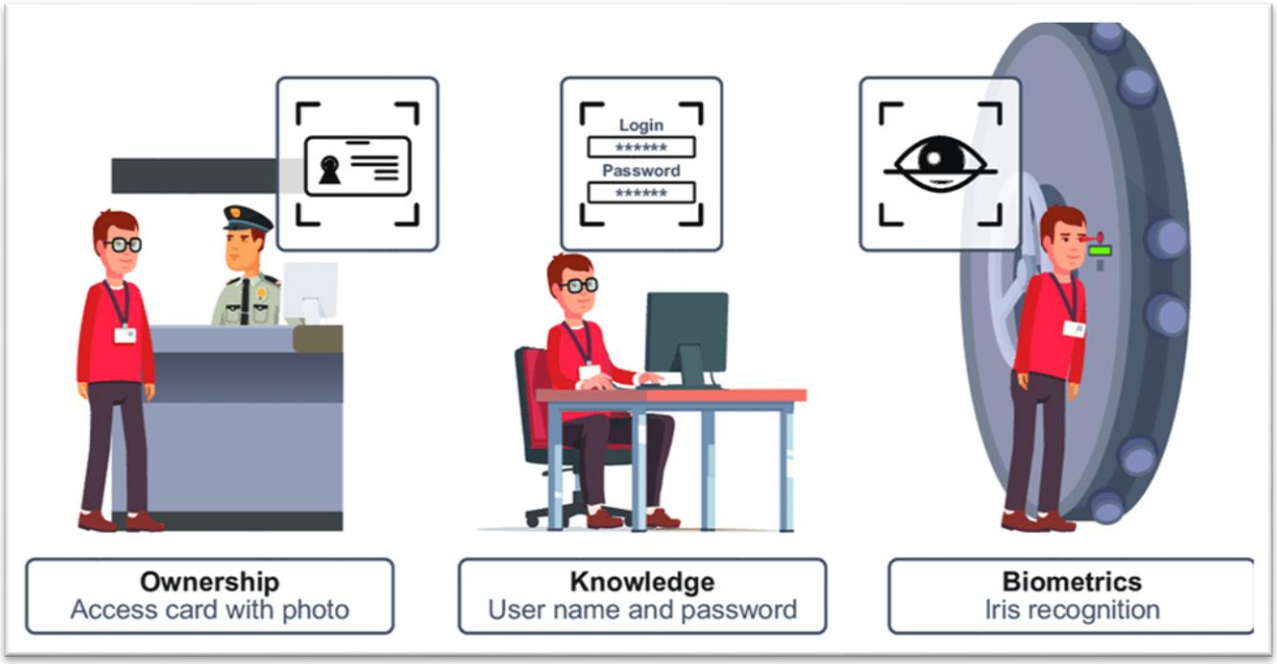

Figure 23: Conceptual authentication examples [49]

There are different levels of authentication used to increase security. Below are defined:

Password-based authentication (Single-factor authentication)

Single-factor authentication is very user-friendly, easy to implement, but there are a number of challenges like the only thing between user and resources is password (something you know factor), it is very easy for the attacker to gain access to the resources as nothing else is there to stop them from getting into the network(as shown in Figure 24) [50].

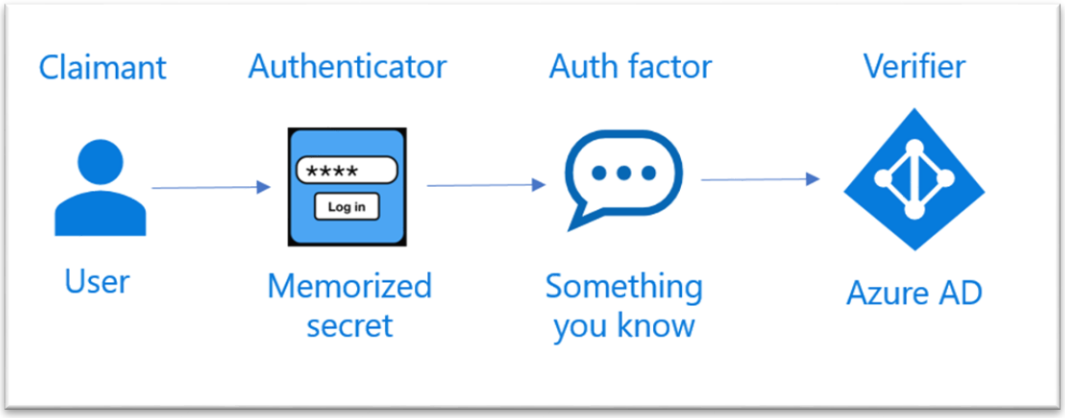

Figure 24: Single-factor authentication [50]

Flow chart of single-factor authentication as shown in Figure 25:[56]

- The user login into any website using the username and password.
- On the server-side, the user database server checks the form submitted by the user.
- If the credentials are correct, the user is authenticated and able to see the display page.
- If the credentials are not correct, the user is requested to enter the credentials again.

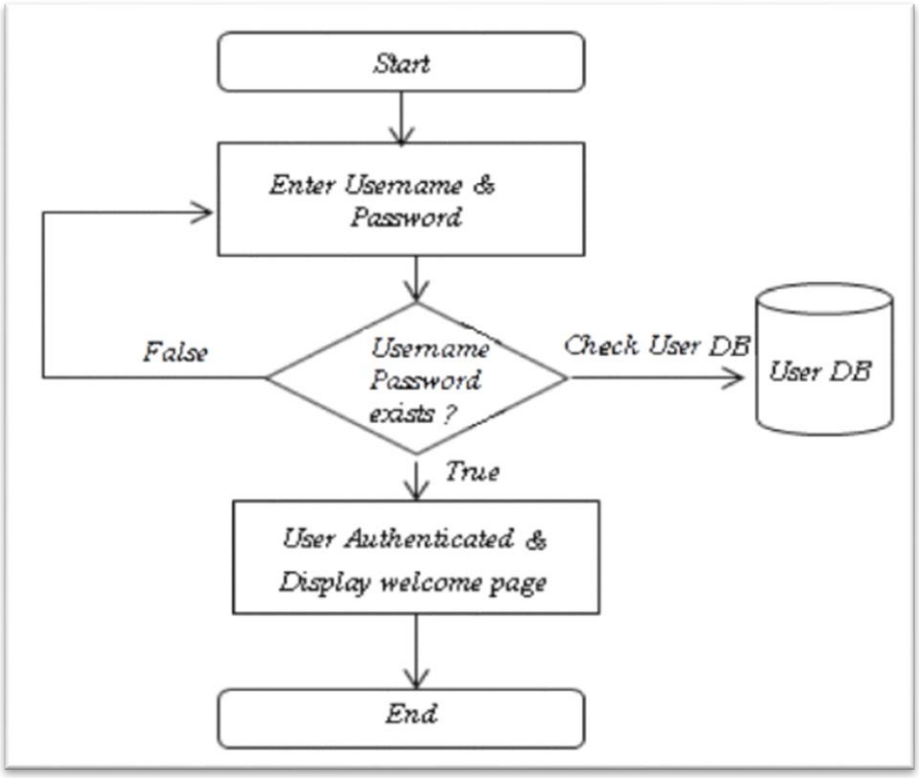

Figure 25: Flowchart of Single-Factor Authentication [56]

However, with the arrival of IoT personal computers, there are many studies [52],[53] that show the weaknesses of this method. Below are some threats to password-based authentication:

- Many users choose easy to guess passwords, share with their friends, write them down in any notebook and use the same password over many social network sites. Also, a large number of users do not change their passwords on a frequent basis.
- An attacker who is interrupting the local communication by sniffing can easily hack the password using malware such as keyloggers or spyware.
- In password-based authentication, knowledge-based systems are used. Therefore, it is very difficult for a user to reset the password, and therefore attackers can use social techniques (for example, there is a number of questions asked, i.e., what is your SSN, what is your last name, personal assets to a user) to take over user's information.

- Attackers use phishing emails (that look legitimate to the user) to urge the user to click on any link and gain access to the password.

In 2011, there were some breaches in Sony and Gwaker that provided a list of usernames and passwords out to the world, and it was found out that 88 emails were the same between them; 92% of them had the exact same password. Therefore, the biggest nightmare of the world is the weak selection of passwords. There is no substitution for the username/password model, but multi-factor authentication (discussed in the next section) was implemented to provide better security against low entropy passwords.

Multi-factor authentication

Multi-factor authentication requires the user to provide two or more authentication factors to verify the identity of a user. Multi-factor authentication verifies a user's identity on multiple authentication factors such as 'Something you know,' 'Something you have,' and 'Something you are.' Two-factor authentication, three-factor authentications are the subsets of multi-factor authentication. As many users normally use short passwords or use common passwords over and over again, that increases the chances of security breaches. Therefore, to enhance the indestructibility of one-factor authentication, two-factor authentication is used as shown in Figure 26 [55]. This method aims to authenticate the individual by using two factors: something you know and something you have.

For example, Password authentication along with hardware/software tokens generated by the code. There are many two-factor authentication products that are available online (some are free while some are paid) like Google authenticator, Microsoft Authenticator and RSA SecureID Access. The main advantage of multi-factor authentication over single-factor authentication is that even if the attacker is able to crack the password, he needs other factors (i.e., card, token) to enter into their account. Nowadays, banks, organizations, Government agencies use MFA widely. OTP (One-time password) is a popular example of MFA in which the user enters the bank password with a new one-time password to access bank records.

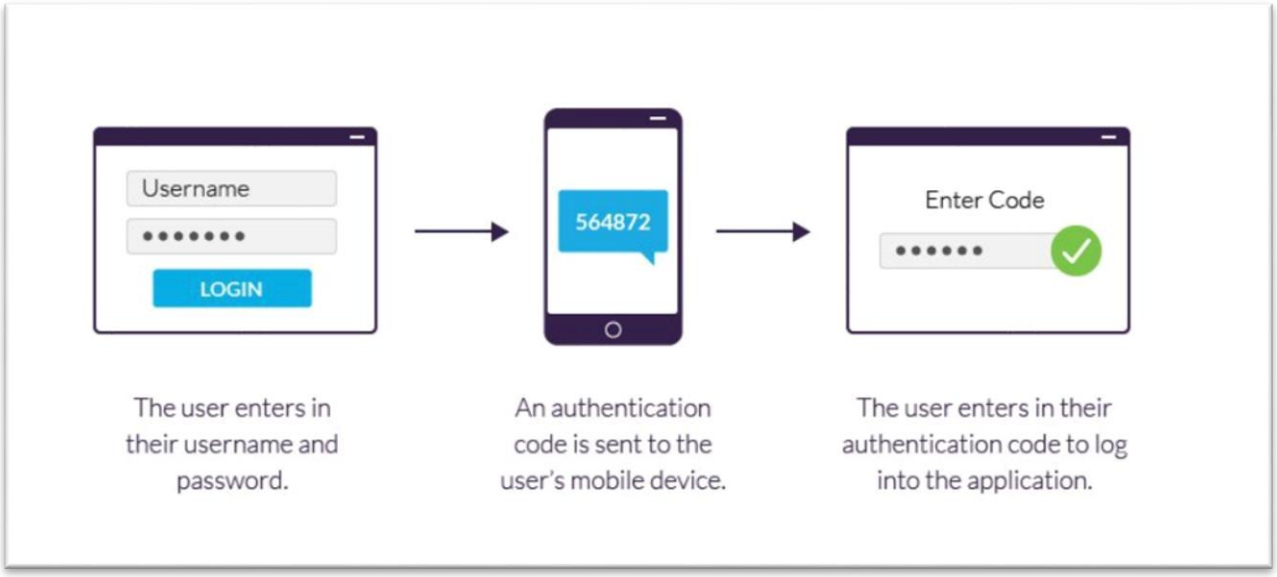

Figure 26: 2FA example using a mobile device [55]

Authentication Flow of OTP two-factor authentication as shown in Figure 27 : [51]

- The user login into any website using the username and password.
- On the server-side, the user database server checks the form submitted by the user.
- If the credentials are correct, the form requests the user to enter the OTP (second authentication factor). If the credentials are wrong, the user is requested to enter the data again.
- If the user enters the OTP, the server-side OTP database verifies the user and grants access.

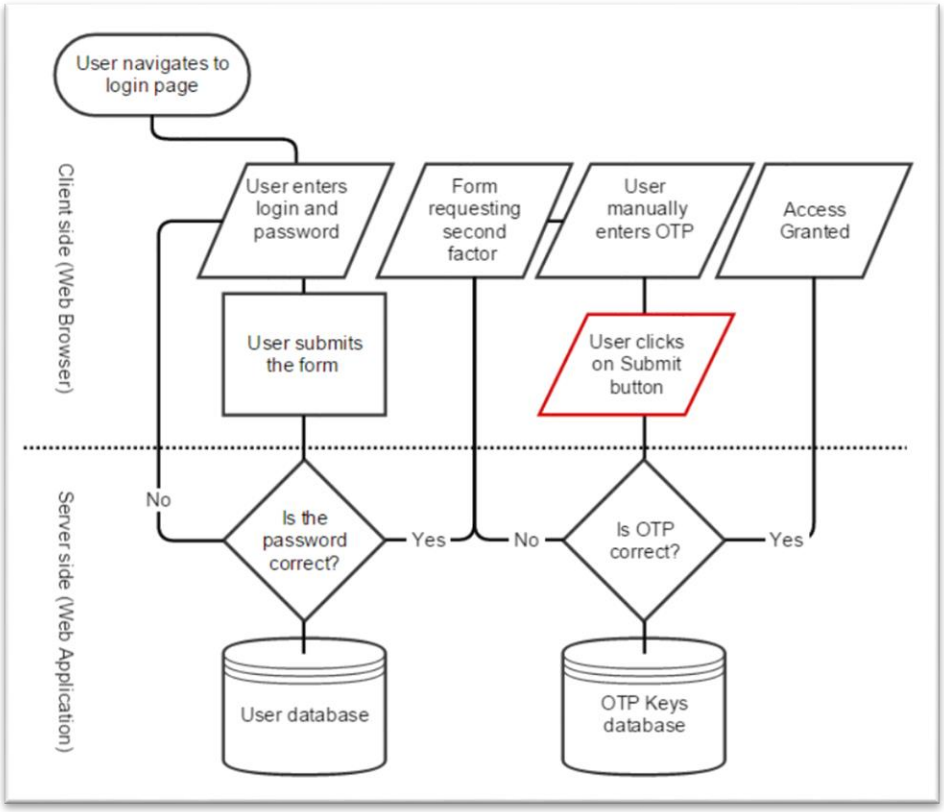

Figure 27: Classic two-factor authentication flowchart [51]

Advantages of Two-factor authentication:[54]

- Increases productivity and flexibility: With the help of mobile two-factor authentication, organizations can secure their sensitive information because employees can access the company's data virtually on any device or location.
- Secures the user data as users can use SMS Two-factor authentication solution while login into their email accounts.
- Access monitoring: Organisations can limit user access to certain applications.

Certificate-based authentication

Certificate-based authentication is used to identify whether a user or device is authorized on the network by a digital certificate. It is based on the authentication factor 'something you have' i.e., the private key and 'something you know,' i.e., password. As illustrated in the figure 28 [57], to authenticate a user to a server, the client sends certificates and data across the network with the

use of an SSL connection. The server authenticates the client's identity on the basis of this evidence.

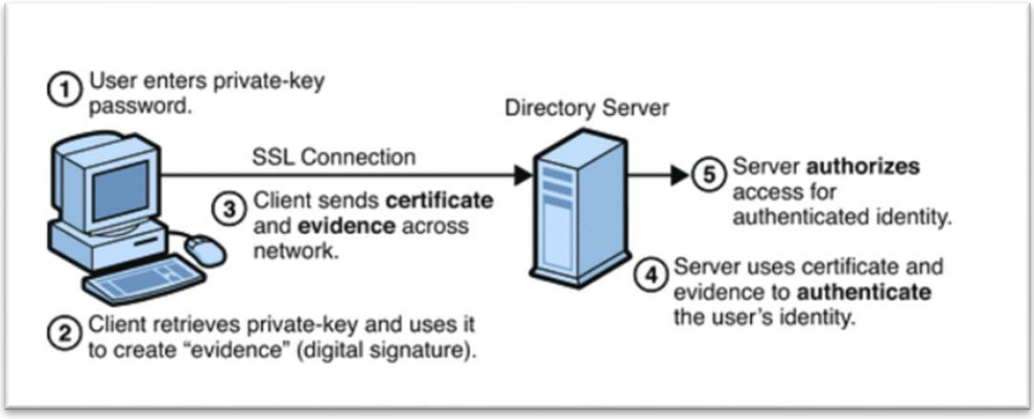

Figure 28: Certificate-Based Authentication [57]

Types of Certificates

- TLS/SSL server certificate: The TLS/SSL protocol makes sure that there is secure communication between client and server. The server authenticates itself by providing a digital certificate [58].
- TLS/SSL client certificate: Client authenticates to TLS service by client certificates. CA (Certificate Authority) issues the certificate containing the username, password, email address to authenticate users.
- Email Certificate: To perform secure email communication, both parties should have sent each other digitally signed certificates in advance.
- Self-signed and Root Certificates: Root certificate is the top-most certificate because the trust of digital certificate starts with the 'root certificate.' A CA self-signs a root certificate to be able to sign other digital certificates.
- There are many other certificates like Role-based Certificate, Group Certificate, Qualified Certificate, Code-signing Certificate and EMV Certificate.

Certificate-based authentication for wireless networks

As the trend of the wireless network is emerging in day-to-day life, one of the major issues is that it is prone to attacks like DDoS, Eavesdropping, spoofing etc. One of the prime importance of such a network is to implement security. In certificate-based authentication, the main advantage is that

it is not limited to server-to-client authentication but can also be applied to client-to-server authentication, i.e., it uses asymmetric cryptography. For example, organizations can determine if the PC A on the network is registered to user A. If yes, then user A is granted access to the network.

In a wired network, a server exists that handles the creation, updating and cancellation of certification. In contrast, there is no timely communication with the certificate server in wireless networks due to dynamic network topology. However, one of the primary concerns in this method is the secure distribution of public keys over the network. Public Key Infrastructure (PKI) is a set of methods developed to support asymmetric (public key) cryptography by creating, requesting, and handling public key management using X.509 certificates. In simpler words, the sender's message is encrypted using the receiver's public key, and then the receiver decrypts the messages using the corresponding private key. X.509 standard defines the certificate format. Moreover, CA was introduced for more trust, which is a trusted party for verifying and creating X.509 certificates.

PKI's Components

Figure 29 shows the PKI's components and defined below:

Certificate Authority (CA): CA is a trusted organization that issues certificates to know who is communicating online[59]. CA also revokes the certificate if there is a loss of a private key.

Registration Authority (RA): RA is managed by only one administrator who can access all the RA functions and add more administrators if want. RA lists all the user information and requests to CA before certification.

Distribution Authority and Certificate Repository: Stores all the certificates and certificate revocation list information.

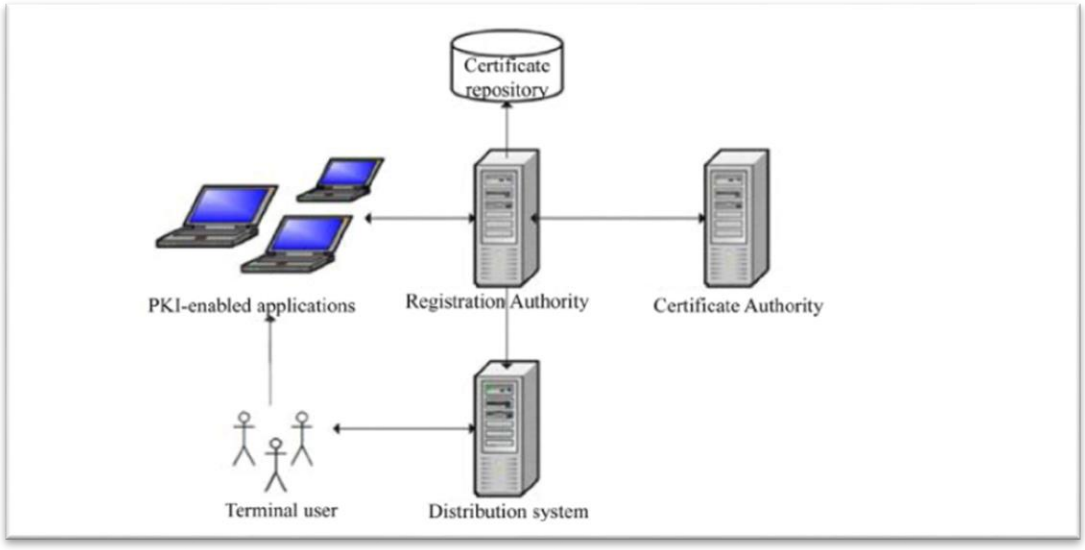

Figure 29: PKI's components [59]

Below is the protocol for certificate-based authentication as illustrated in Figure 30 [59]:

- In the first step, the Registration Authority (RA) passes the user identity with public key to CA for certificates. Then, CA (Certifying Authority) issues a certificate to the user, device or machine, consisting of much information like issuing time, expiration time etc. The certificate is created by CA using the user's IP address, name, or public key.
- During the second step, the CA renews all the non-expired or revoked certificates and sends them to Validate authority.
- The third step is the signature generation, where the user sends a message with a public key certificate including signature data.
- The fourth step is certificate validation which is done by either checking the CRL(Certificate revocation list) list or inquiring the Validating authority.

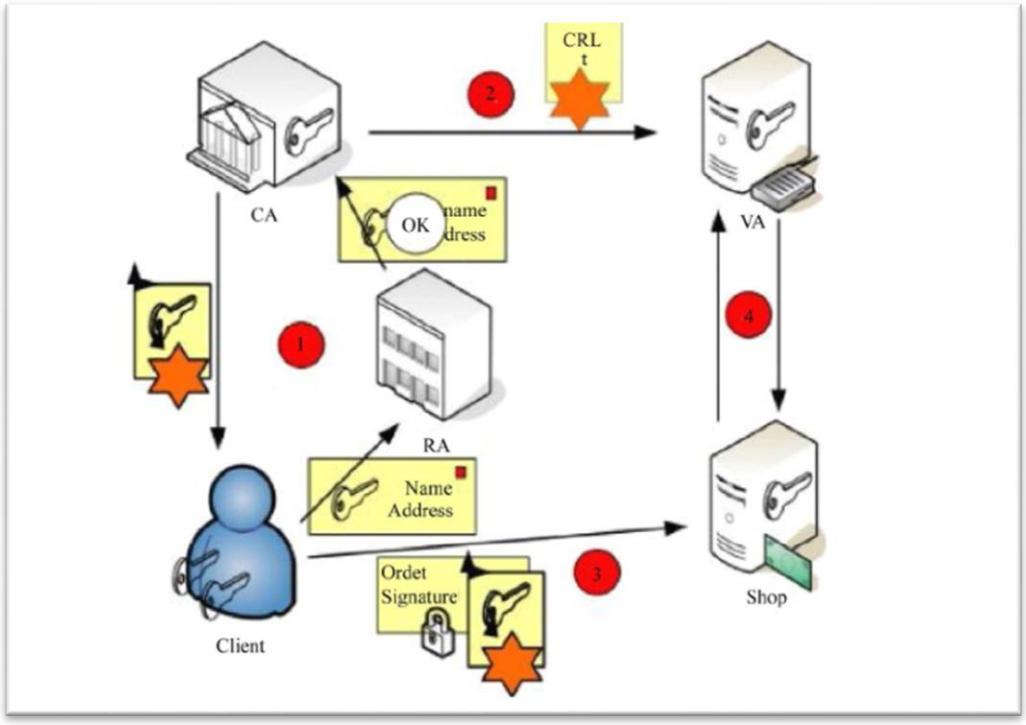

Figure 30: Protocol operations and actors of the PKI [59]

Flow of Certificate-based authentication

The administrator generates and assigns certificates to devices in the organization [59]. The administrator configures his active directory to trust specific users by importing digital certificates of the users. The devices are also trusted by importing server certificates. Now when a user wants to log in to the network, an access request is sent from the user's device into the network server. This handshaking process between the network server and device continues until both are completely satisfied that the credentials are correct. In this method, a Digital Certificate is represented by 'something you have' authentication factor besides username and password(Something you know).

How Certificate-based authentication meets the needs of an Enterprise

Organizations need a strategy that implements agility, revenue, and flexibility but at the same time should consider the business risks, how to secure the data and mitigate the risks [60]. Certificate based-authentication provides multi-factor authentication without staggering burdens on employees. Moreover, Certificate-based authentication provides authentication and access management requirements because, in today's world, all users use multiple devices while working, travelling or eating. This method can be used on multiple platforms and can be easily deployed to

desktops and smartphones. A best practice is that Certificate-based authentication provides multi-factor security without burdening the users to carry additional devices and keeping the technology dynamic and mobile.

Certificate-based authentication meets the requirements of the following compliance:

- HIPAA(Health Insurance Portability and Accountability Act): In 2003, HIPAA announced the 'security rule' to protect and secure health insurance and electronic health records. All the organizations (health care industries and insurance companies) that contain the data should implement the Security rule. Certificate-based authenticate meets this requirement by ensuring authorized users access electronic health records.
- PCI-DSS (Payment Card Industry Data Standard Security): The payment card industry published the PCI Data Security Standard in 2004 to prevent credit card fraud or losses. Organizations storing sensitive data should contain at least one of the authentication factors ('something you know,' 'something you have,' 'something you are') or should use multi-factor authentication while accessing the data across the remote network. Certificate-based authentication fulfills this requirement.
- FFIEC (Federal Finance Institutions Examination Council Authentication Guidance): FFIEC also focused on implementing security features that match customer acceptance, scalability, and interoperability. Certificate-based authentication satisfy this requirement because there is mutual authentication between client and server which also provides defence against phishing, DOS, or similar attacks.

There are many risks and challenges in PKI. As we know that the PKI is a pair of public and private keys. Frauds can happen if the private key of the customer or CA is stolen. There are two ways to mitigate these risks; one way to protect the private key is to use a strong combination of passwords (not easily guessed). Another way to protect the private key is by using a smart card which is a one-time unique password. Although there are many risks still involved, PKI is a good solution at the present time. It uses pair of public/private keys, hashing algorithms, digital certificates to reach a goal of security and confidentiality of user data.

Biometric authentication

Biometric refers to the identity verification of a human by analyzing a person's characteristics. It is based on authentication factors, 'something you are or 'something you do.' This improves the security feature of the application, as a person does not have to remember a password or hold any token. An excellent biometric feature should possess the following characteristics [61]:

- Performance: A successful recognition must be in the required time and should be accurate.
- Acceptability: Users should not feel defensive and accept the system comfortably.
- Distinctiveness: This is an essential feature as any two individuals should be different enough to separate their characteristics.
- Universality: Each individual should possess the trait.
- Collectability: A trait should be attainable and measurable.

A biometric system, after extracting biometric data operates in two modes as shown in Figure 31:

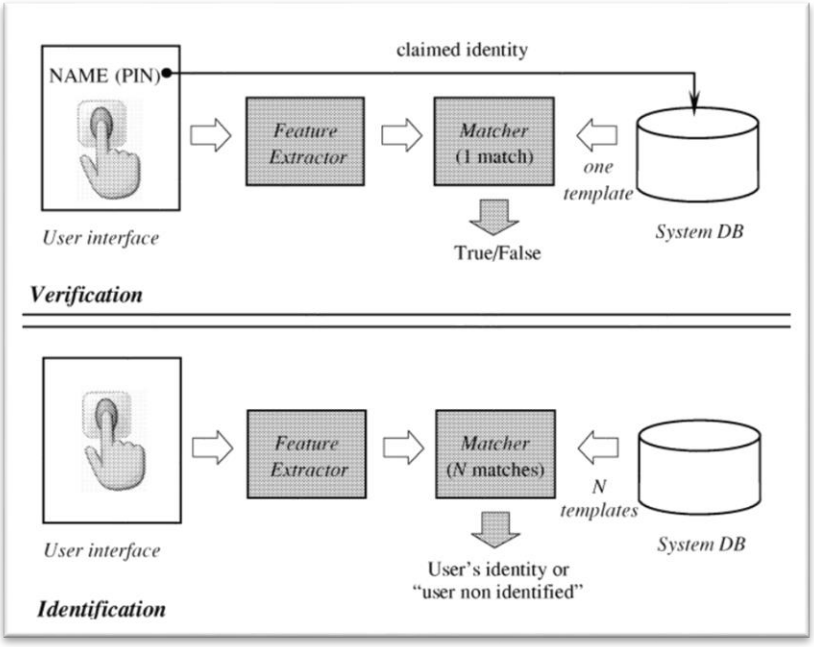

Figure 31: Block diagrams of verification, and identification tasks [61]

- Verification Mode: The main focus of this mode is to prevent multiple people from using the same identity. The system compares the user's biometric data (PIN, Smart card

information) with the biometric sample stored in the database to determine whether the users are what they declare to be.

- Identification Mode: This mode uses one- to -many approach for comparing an individual's identity by searching the templates of all the users in the stored database for a match. There are two sets of identification; the first is 'closed set identification,' where the system recognizes the user under a predefined list. The second is 'open set identification,' where the users are not in the database.
- Feature Extraction Module, in which the attained biometric data is processed to extract noticeable features.
- Matcher Module, in which the comparison is made through extracted data and stored templates.

Biometric traits can be broadly classified under two categories as shown in Figure 32:[63]

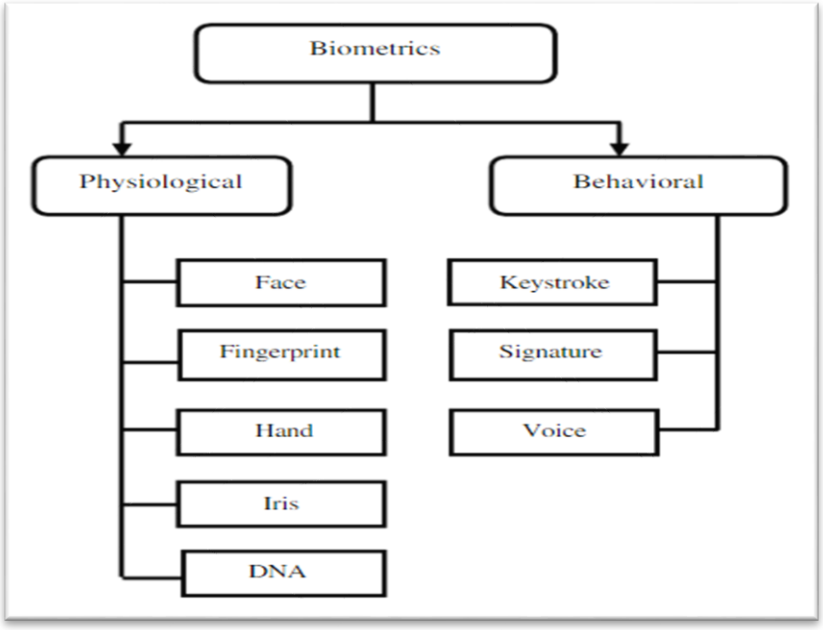

Figure 32: General block diagram of Biometrics system [63]

Physiological Biometrics

It is directly measured on the part of the human body that does not change with time. These are subclassified into:

Face Recognition

Facial Recognition is a technique of automatically verifying a person from a still image or video. It depends on two areas, facial metric and eigenfaces. The facial metric technology looks for the position and distance of eyes, nose, eyebrows, lips, and mouth as shown in Figure 33.[64]

Figure 33: Biometric Facial Recognition [64]

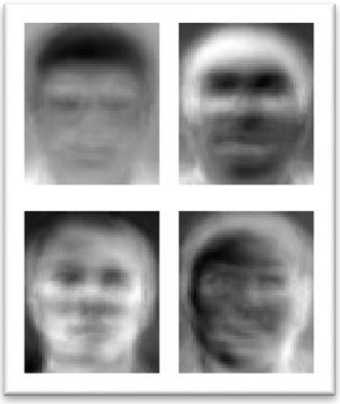

Figure 34: Eigenfaces [65]

In the Eigenface method (as shown in the figure 34 [65]),the machine learning algorithm is used to reduce computation and complexity by determining a variation of faces in a collection of face images and using those contradictions to decode or encode a face. However, there are some challenges in this method, like if there is a restriction on the image like black, white background, fixed illumination; however, problems with lightening, various facial expressions or a person wearing eye-glass, hat, a scarf can degrade the performance. In order for a facial recognition system to be successful, it should recognize the face from any angle.

Fingerprint Recognition

This method is the oldest and most established method today because there is the probability that two persons having the same fingerprint pattern are one in one billion. It detects the identity of a user by looking at the fingertip patterns. The matching is performed using minutiae-based fingerprint matching in which fingerprint image is first enhanced using Fast Fourier Transform and then converted to a binary image for further processing. In the last step, the image is thinned, and details are extracted. There are some problems with this system like some people are not suitable for this, e.g., manual works having a large number of cuts on their fingertips. Other factors are aging, genetic reasons or environmental factors. Figure 35 shows the minutiae-based extraction in fingerprint recognition. [66]

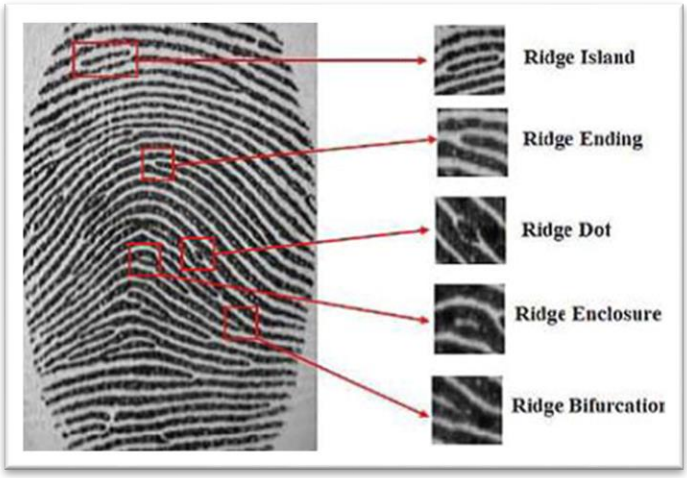

Figure 35: Some common minutiae patterns [66]

Hand Recognition

In this method, hands and fingers contain structural geometry with unique dimensions for every person that cannot be changed. In this, different measurements are taken from hand like palm size, the shape of the hand, length and width of fingers. There possess some challenges in this method, like, hand geometry in children is not constant during their growing age, some people wear rings, problems like arthritis can pose further challenges in extracting correct hand geometry information. Figure 36 shows a contour-based extraction scheme:[67]

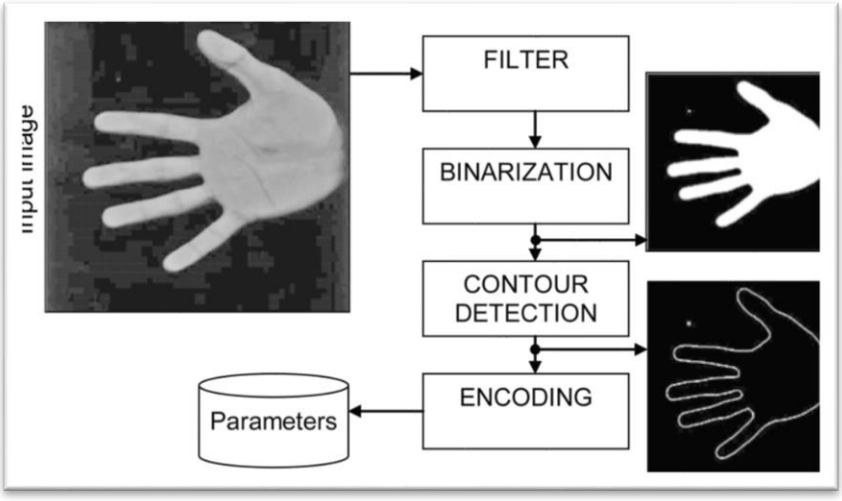

Figure 36: Block diagram for the proposed extraction scheme [67]

Retina Recognition

This approach uses the low-intensity coherent light source by analyzing the blood vessels pattern because blood vessels have a unique pattern from eye to eye. This method requires the user to place their eye close to the scanner and focus on a location for at least 10 to 15 seconds while the iris scan is complete and used as a biometric template for the authentication process of individuals. The error rate in this scan is very low because it is impossible to form a human retina, and also, the retina of a dead person decays too rapidly. However, the challenge in this approach is that any person wearing a lens or glasses becomes difficult in distinguishing the person. Figure 37 on the left side shows the retina scan. [69]

Figure 37: On the left is a retina and on the right is an iris image [69]

There is a difference between retinal and iris scan, i.e., retina scan is more accurate. In the IRIS scan (right figure), the system captures the complex pattern of the iris, which is a coloured muscular ring surrounding the pupil. However, eyeglasses, contact lenses, watery eyes can decrease the efficiency of this scan.

DNA Recognition

DNA stands for Deoxyribonucleic acid, and it requires samples like hair, blood, semen, saliva etc., for the identification process. This is not a good approach for biometrics because it requires more time to process the result and is not automatic. It is widely used in law enforcement offices and forensic applications.

Behavioural Biometrics

It is measured by the action performed on the user.

Keystroke Recognition

This is a behavioural characteristic of humans by examining the speed and pressure taken by a person to type the password or any typing pattern. It is done by hitting the keys on the keyboard. There are many other behavioural biometric techniques like signature and voice recognition.

Biometrics Performance evaluation

The performance evaluation of biometric systems depends on the following metrics:[68]

- False Match Rate (FMR) or False Accept Rate: It measures the percent of invalid matches when a system incorrectly peers an input with a non-matching template pattern in the database.
- False Non-Match Rate (FNMR) or False Reject Rate: It measures the percent of valid matches rejected by the system as it discards a valid input with a matching template pattern in the database.
- Equal Error Rate or Crossover error Rate: The value of ERR is obtained from the ROC (Receiver operating characteristics) curve (trade-off between FMR and FNMR based on a threshold) at which the acceptance and rejection errors are equal. A device with the lowest ERR is the most accurate. Figure 38 shows IRIS biometric system is the most precise [62].
- Failure to Enroll Rate: This rate is caused when data quality is poor, and the system fails to accept the data.
- Failure to Capture Rate: The rate when the automatic systems fail to accept the data even if presented correctly.
- Template Capacity: Maximum number of template sets stored in the database.

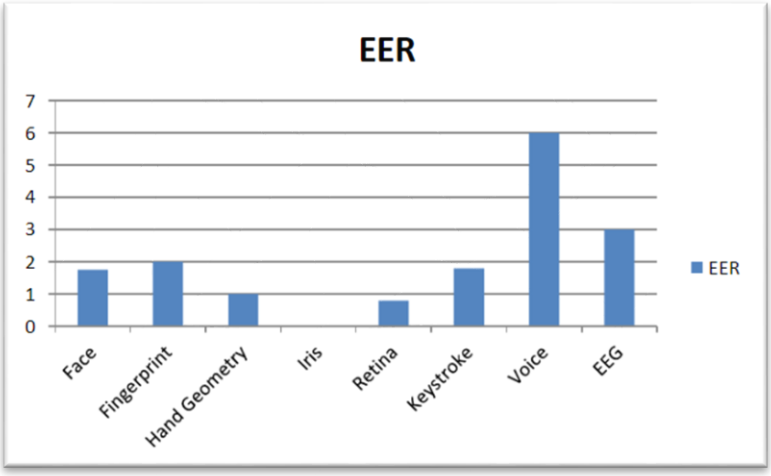

Figure 38: The Equal Error Rate (EER) for different biometric systems [62]

Application of Biometric Systems in Various Enterprises

The applications of biometrics in different organisations can be divided into three main groups:[61]

- *Government*, biometric applications include driver's license, social security number, national ID card, passport control and welfare-disbursement control.
- *Forensic*, biometric applications include parenthood determination, missing children, criminal investigation, terrorist identification and corpse identification.
- *Commercial*, application includes Internet access, ATM, credit card, physical access control, cellular phone, medical records management, electronic data security, computer network login and e-commerce.

Many biometric application are deployed in large civilian application. For example, the Schiphol Privium scheme at Amsterdam airport has employed iris scan cards to speed up the visa and passport control procedures. Passengers enroll their card and look at the camera; the camera computes the Iris code to match it with data in the card for user verification. Therefore, biometric systems are being used by many enterprises to improve their security.

Single Sign-On

In a single sign-on, the user can authenticate an application once and access it multiple times without login in again [70]. Once an identity provider authenticates the user, they can access the applications as long as their session is not expired. There are multiple scenarios when a user is using Single Sign-on. For example, when a user uses any random application, it allows them to log in via Google sign-in. Another example is using single sign-on in universities by students, professors, and administrators to access university applications. There are many benefits of using Single Sign-On listed below:

- Users enjoy single sign-on as they don't have to authenticate again and again. Also, they don't have to remember all usernames/passwords, and there is no disclosure of credentials to applications.
- Single Sign-on also provides an advantage to the organization by implementing the authentication policies, account recovery, account termination and logging for multiple applications in a single place.

- In the case of single Sign-on, Application owners can trust identity providers for validation of login pages, secure storage of credentials and account recovery.

However, with a single Sign-On, there are some trade-offs also:

- Single Sign-on creates a gateway to all the applications, which can cause a single point of failure.
- Single Sign-on also uses a centralized service that can cause a single point of attack.

To mitigate these risks, whenever an organization selects an identity provider, it should perform an in-depth evaluation of all the privacy features and security controls before trusting the provider with its applications. Also, organizations should select an identity provider that is highly available and maintains the confidentiality of users because it tracks all the user activity across all sites.

Single Sign-On Authentication Methods

Security Assertion Markup Language (SAML) 2.0

New SaaS applications created difficulties for managing identities as there was no efficient way to manage employee identities. The organization was also facing difficulties in tracking its employees, and users needed to remember the password for each application. Finally, in 2005, SAML (Security Assertion Markup Language) 2.0 was introduced to solve single web sign-on across different domains. Also, using SAML 2.0, SaaS applications could redirect employees back to their identity provider for authentication. However, one major problem with SAML 2.0 was that it only authenticated users based on application but couldn't authorize users based on APIs.

OpenID Connect

OpenID Connect was designed to convey the identity of a user to the application securely. It is built on the OAuth 2.0 protocol and provides both API authorization and user authentication.

OAuth 2.0

With the rise of social media, many users want to upload pictures. For this, applications need to fetch such images on the user's behalf. For example, a person uploads a photo on social media (such as Facebook, Instagram). The person then wants to access that photo (which is on social media site) from a website that prints the image. If there is not a good solution, the user has to

share his username/password with the website that prints the photo. There is a significant risk associated with it if the photo printing website is compromised.

OAuth 2.0 is a solution to this use case. It allows the user to authorize an application at one site (client: photo printing website) to fetch their picture from another site's API (resource server: social media website)without exposing their credentials. For example, many consumer-facing applications nowadays retrieve users' information from LinkedIn profiles.

Working of Single Sign-On

Single sign-on works on any authentication protocols discussed above to authenticate a user. Figure 39 shows a typical example of the working of a Single sign-on. In this example, a user visits application 1, redirecting the user to Identity Provider A for authentication. The Identity provider A then authenticates the user, sets up a session for the user, creates a cookie in the user's browser with session information. After that, Identity provider A redirects the user's browser back to application 1 with a security token containing the authentication event and authenticated user information. If the user then visits application 2, it redirects the user to Identity provider A. The user's browser has identity provider A's cookie, so the Identity provider uses the cookie and detects that the user is already authenticated. Then it checks if the authenticated session is still valid; if it is valid, the user's browser is redirected back to application 2 with a security token without prompting the user to enter the credentials. However, if the session is not valid, identity provider A will prompt the user to re-authenticate. Therefore, SSO enables a person to access multiple applications while authenticating only once until the session is not expired.

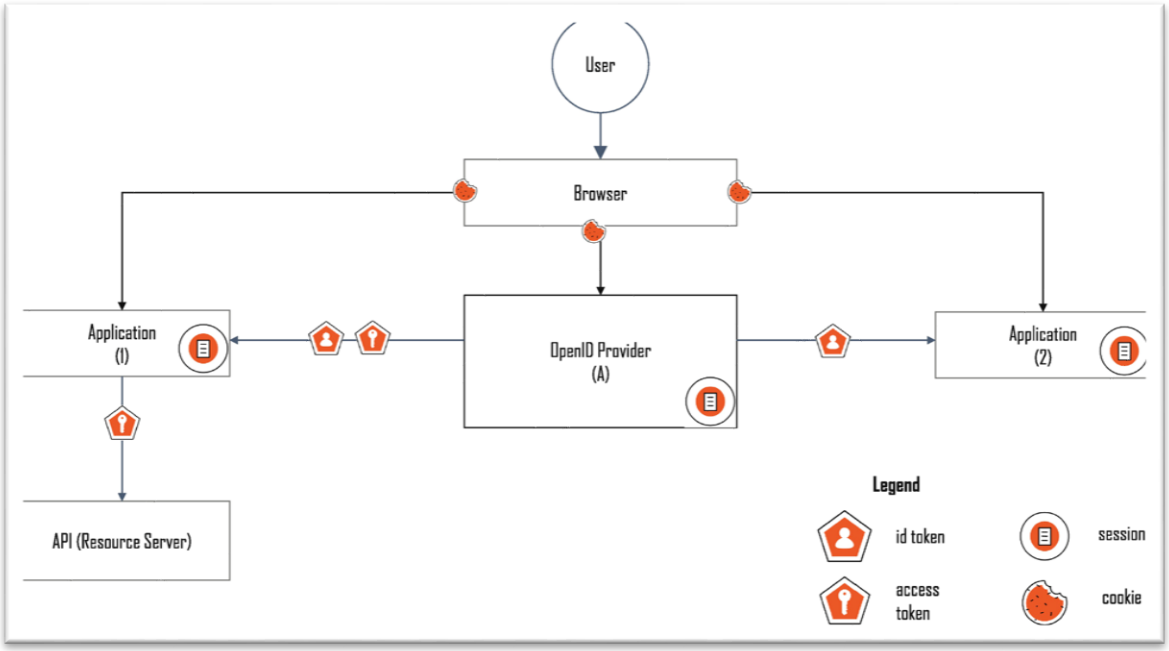

Figure 39: Single Sign-On [70]

For example, Google implements Single Sign On in its services. Google's central server is https://accounts.google.com. Once a user is logged into this server, user will be able to access Gmail, YouTube, Google maps and Google Docs without entering the credentials again.

Multiple Identity Providers

In the below scenario illustrated in Figure 40, Single Sign-On is implemented using an authentication broker that allows the configuration of multiple identity providers. The authentication broker should be configured in such a way that it allows only users to access applications appropriate to them. For example, as illustrated in the diagram, an authentication broker should ensure that employees cannot get access to those applications intended for partners and vice versa. Application 1 should be only accessed by employees authenticated by Identity provider A and Application 2 should be only accessed by partners authenticated by Identity provider B.

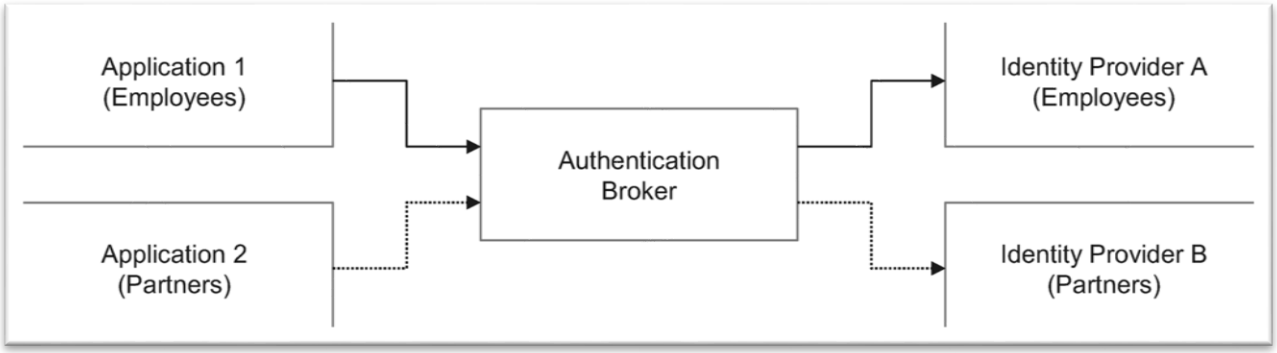

Figure 40: Authentication Broker with Multiple Identity Providers [70]

Zero Trust Security Model

Need of Zero Trust Security Model

As the cybersecurity threats are growing in number, the National Institute of Standards and Technology (NIST) took all the major factors, including pervasive mobility and big data analytics, to create a different approach to cybersecurity. The result was a 'zero trust model' for information security. Below are a few basic causes for the need for a zero-trust security model [71]:

- Traditional security models were based on the concept of the 'trust but verify' approach. The approach was based on the trust that DMZ network segmentation using VLANs can create a boundary between trusted and untrusted networks. But this approach is not feasible in a modern cloud computing environment and mobile platforms. Therefore, an explicit model was proposed to provide dynamic security policy but also places micro-segmentation and isolation of critical elements. The zero trust model is based on the approach 'never trust, always verify,' in which all the traffic (even between Virtual machines) is validated.
- Due to a high wave in technology, like a corporate company having multiple internal networks cloud-based applications, remote network infrastructure is growing complex. Also, people are migrating from personal computers to the use of mobile phones. However, these devices are vulnerable to threat and cannot be easily secured with perimeter-based network security as there is no single perimeter. So, protecting these devices is important to secure the identity of the owner. There are approaches like Cryptographic File System (CFS) and persistent authentication, which are installed in the existing systems (PC's) to protect the information. However, there are some disadvantages in CFS, like the decryption key is held back into the system, which can be used to extract the real data. In persistent authentication, the user is forced to enter the password every time he logs into the system, which can be really frustrating and increases the burden. These complicated cases have led to the development of Zero Trust Security Model (ZTSM).

Introduction

Zero Trust Security model, also known as perimeter less security, supports mutual authentication by providing authentication, authorization and encryption between users, devices, and applications. It was established by John Kindervag, an industry analyst at Forrester. The implementation of ZTSM is based on the concept 'never trust, never verify,' which means[72]:

- ZTSM must be able to defend against the internal and external threats on the network all the time.
- Never trust a device, even if it is on a corporate LAN or previously verified.

The initial focus of this model is to provide Just in Time access, i.e., providing minimum privileges to carry out any task. Another focus is to avoid exposing sensitive data. For this, a wireless token that is unambiguous to the user performs the authentication on the user's behalf to maintain the confidentiality of the system. When the user leaves the system, the state of authentication changes to unauthenticated as there is no token, therefore this model builds trust between tokens and devices, giving the authentication to only trusted devices without affecting the machine's performance. The goal of zero trust security model to provide security while reducing the user's involvement. Figure 41 shows a zero-trust access model, in which a user on his local machine needs access to enterprise data and the access is granted through PDP/PEP gateway, i.e., Policy Decision point and corresponding policy enforcement point.[73]

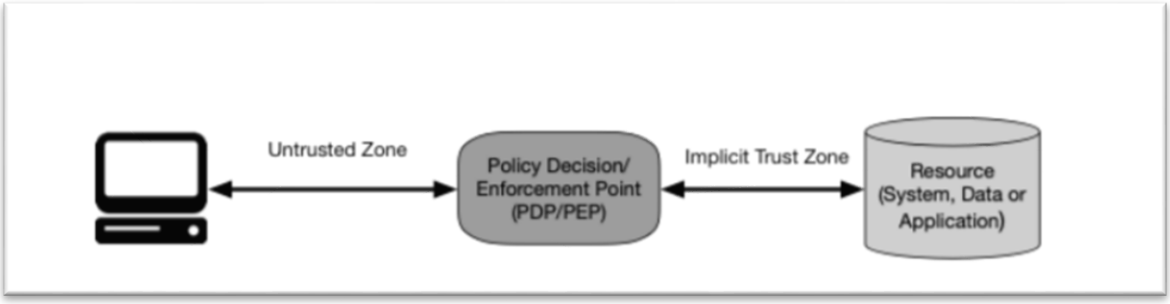

Figure 41: Zero Trust Access [73]

NIST Zero-Trust Architecture

Figure 42 shows Zero Trust logical components and their interaction that are involved in the deployment of service, whether on-premises or cloud in an enterprise. Policy Decision Point is

broken into Policy engine, and policy enforcement point. The architecture uses a separate data plane and control plane.[73]

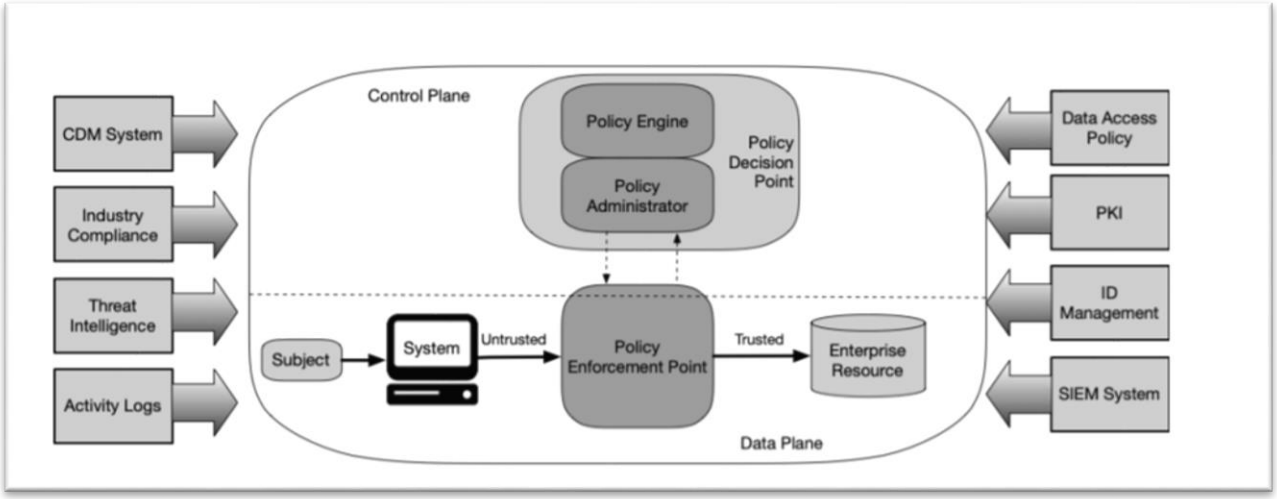

Figure 42: Core Zero Trust Logical Components [73]

Description of all the core components:

- Policy Enforcement Point (PEP): PEP systems acts as a logical component for enabling, monitoring and terminating communication between subject and enterprise resources. PEP is also responsible for forwarding and receiving policy updates from the Policy administrator.
- Policy Engine(PE): The policy engine is coupled with the policy administrator. The policy engine component creates and logs approved/denied decisions while the policy administrator executes those decisions. Policy Engine uses CDM(Continuous diagnostics and mitigation) systems or threat intelligence services to give the ultimate (grant, deny or revoke) decision.
- Policy Administrator(PA): It is paired with PE and relies on its decision. PA component generates session-specific information(authentication token or credentials) used by the client. If the session is authorized, PA sets up PEP to start the session. If the session is unauthorized, PA signals PE to shut down the communication between the client and enterprise resource.

In addition to logical core components, there are several local and external data sources that are used by the policy engine while making access decisions. These include:

- Data Access Policy: These policies are used to provide basic access rights to user accounts, applications, services in an enterprise. It contains a set of rules, attributes and policies created by a policy engine to provide access to enterprise resources.
- Public Key infrastructure (PKI): This component is responsible for creating and logging enterprise certificates to the subject, services, applications, and resources.
- ID Management: This component is used for storing, creating, and managing both enterprise and non-enterprise user accounts. It works with another component such as PKI to get all the necessary information such as name, email address, role, certificates.
- Security Information and Event Management (SIEM) System: This component collects all the logs and event data generated by the enterprise for security analysis.
- Continuous Diagnostics and Mitigation (CDM) System: CDM systems gather information about the organization's current state and provide continuous updates to the policy engine.
- Industry Compliance: This component makes sure that while making policy rules, the enterprise remains cooperative with any of the regulatory regimes that it may fall under.
- Threat Intelligence: Threat intelligence includes information like newly discovered attacks, vulnerabilities, flaws, malware from all internal and external sources so that the policy engine will deny access while making decision rules.
- Activity Logs: This system combines all the network traffic and asset logs in real-time that provides feedback of the enterprise security posture.

Zero Trust Security Model in Cloud Computing Environment

Cloud computing technology has seen rapid growth in recent years as it lessens the burden of installation, licensing, training, and maintenance. Trust is an important measure provided by cloud service providers to cloud users. Below defined are some trust challenges faced in a cloud environment:[74]

1. There are many trust evaluation techniques such as Black-box, inside-out, outside-in. But all these approaches have a different techniques for trust evaluation. Therefore, an efficient approach needs to be built for the cloud paradigm.

2. For trust establishment, qualitative and quantitative information needs to be examined from distinct roots to build a trust model. How information is combined from different roots is a major challenge in a cloud computing environment.

3. In a cloud environment, one major challenge is to differentiate between global trust and local trust while defining parameters for entities.

Therefore, a zero trust model is the best fit for the cloud environment. The zero trust model is about eliminating trust from a system rather than considering a system as trusted as cloud environments are dynamic and sharable. Zero Trust security model supports technologies such as Identity and Access Management (IAM), data encryption, multi-factor authentication for both on-premises and cloud resources. Figure 43 shows the basic concept of the Zero-trust strategy:

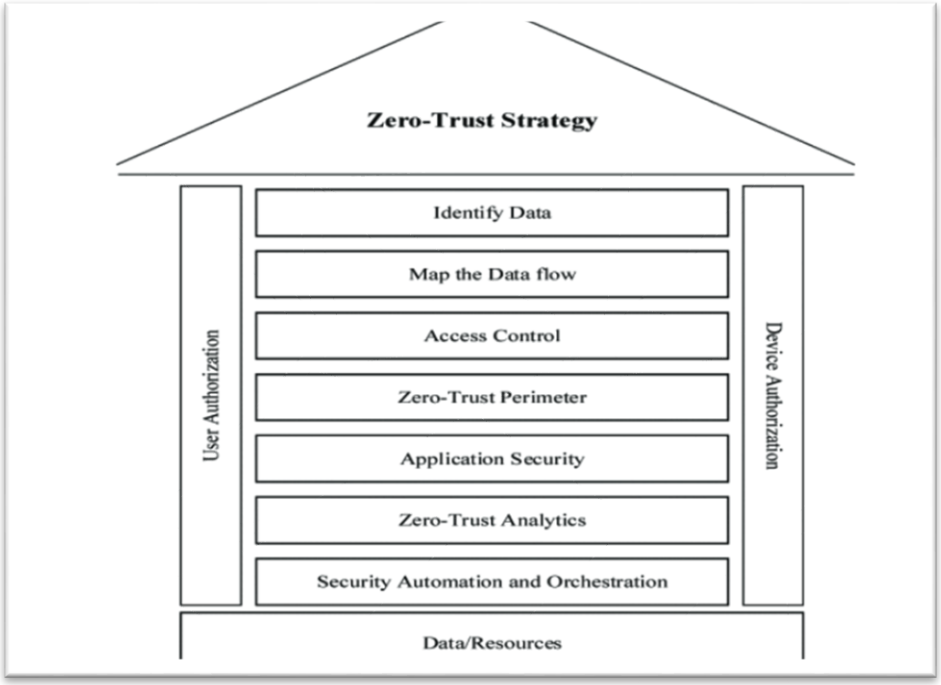

Figure 43: The basic concept of Zero-Trust Strategy [74]

The main objective of zero-trust architectures in a cloud environment is to protect cloud service providers from cyberattacks. To more understand the zero-trust approach in the cloud, below are some principles defined:

1. Identify Data: The very first step is that Cloud service providers should identify sensitive data(PII, health information, payment card data etc.) in cloud service.

2. Map the data Flow: The second step is to observe the multi-directional flow of sensitive data across all the small networks.

3. User Authorization: In this, end users are authorized through IAM, MFA etc. However, access requests are monitored continuously to validate the users.

4. Device Authorization: All the devices connecting to cloud environments are validated through Device Managers.

5. Access Control: The main principle of this rule is to limit access in cloud environments to protect from insider threats.

6. Zero-trust Perimeter: Once the flow of data is mapped and all the above steps are done, an optimal micro-perimeter is created by deploying a next-generation firewall to allow only legitimate traffic to access the protected surface.

7. Application security: For this factor, MFA is the best approach to adopt zero-trust.

8. Zero-trust Security Analytics: This step involves the use of strong security analytics to analyze logs in real-time and place the most intelligent defences.

9. Security Automation and Orchestration: This step involves implementing various automated tools to perform tasks across cloud environments.

Zero trust Multi-Cloud Use Case

Nowadays, multi-cloud is a common use case that enterprises are using with Zero trust Architecture. As represented in Figure 44, an enterprise has a local network but uses two cloud service providers to host applications, services or data. For overall flexibility, an application hosted on Cloud provider A should be able to communicate directly with an application hosted on Cloud Provider B without going to the enterprise network. The approach to this use case is:

- Place a Policy Enforcement point at access points of each application.
- PE and PA services should be located on any one of the cloud providers.

This way, an enterprise can still manage resources even if hosted outside the enterprise network. One main challenge with this approach is that each cloud provider has a unique way of implementing a functionality. Therefore, architects need to be aware of how to implement ZTA with each of the cloud providers.[73]

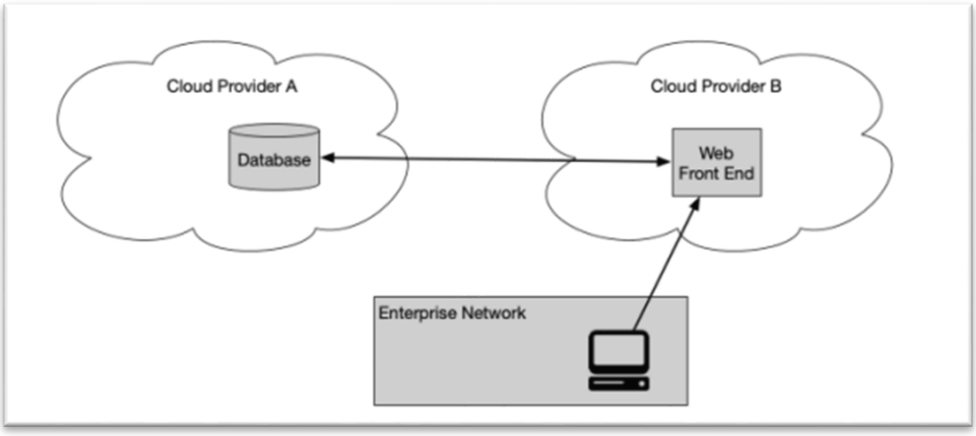

Figure 44: Multi-cloud Use Case [73]

Threats Associated with Zero Trust Architecture

ZTA can reduce overall risks when compared to existing cybersecurity policies and guidelines. But no enterprise can reduce 100% risk; below are some threats related to ZTA:[73]

1. In ZTA, no communication between enterprise resources occurs unless it's approved and configured by the policy engine and policy administrator. Therefore, if a compromised PA or PE allows access to unauthorized resources, a risk occurs. To mitigate these risks, PA and PE should be properly monitored and configured, and any changes in the configuration had to be recorded and audited.

2. Storage of system analysis components like monitor scans, network traffic, metadata etc., are becoming a target for attackers. If an attacker gained access to this network information, they could gain access to enterprise assets and architecture. To mitigate this threat, all the enterprise monitoring and analysis data should be protected.

3. In ZTA, enterprise resources cannot communicate with each other without PA's permission and configuration action. If an attacker interrupts the PA, i.e., perform a DOS attack on it, enterprise operations will be adversely affected. To mitigate this attack, PA could reside in a secure cloud environment.

Cybersecurity In a Hybrid working Environment

Challenges of Managing Cybersecurity at COVID-19

The emergence of COVID-19 and the work from home adjustments in organizational networking left the door to many vulnerable cyberattacks. Moreover, managing cybersecurity incidents during the COVID-19 pandemic was challenging due to many reasons [75]:

Firstly, due to the spread of the virus at a very fast speed, the administration was limited, due to which it was difficult to use a coordinated cybersecurity approach, and the focus was more on a self-help cyber defence. Counselling in handling cybersecurity consequences was either non-existent or lacked the feasibility of an organized cybersecurity approach. This situation made it easier for the attacker to exploit the data of an organization. Therefore, each organization made efforts to develop a global-scale emergency data protection strategy. Also, the fear of disease was so bewitching that cybersecurity experts struggled to keep themselves safe and also develop a solution to protect the computer network.

Secondly, the main challenge was the human factor. Many people are an easy target to social engineering attacks in which attackers use web portals and email scams embedded with malware. Due to coronavirus panic, every information created on the internet created panic, and people click over each website to find the update related to curing, vaccine solution. Cybercriminals took advantage of people's fear and desperation to spread malware.

Below table shows various COVID-19 intrusions related to cybersecurity risk and threats:

INTERVENTION	**RELATED CYBERTHREATS AND RISKS**
COVID-19 Quarantine	Spear phishing email, ransomware, password cracking, cyber espionage, phone scam etc.
Tracking and contacting suspected person having close contact with coronavirus infected person	Social engineering, cyber bullying, cyberstalking, phone hacking, website hijacking etc.
Social Lockdown	Man-in-the-middle attack, Eavesdropping, identify theft on social networking site, social engineering etc.
Border close and travel ban	Website Hijacking, Cloned website, spear phishing email etc.

Wearing of face masks or shields	Confidence trick, fake news, shoulder surfing, cyber stalking, ransomware , impersonation etc.

Identity and Access Control Challenges

Authentication: It is the process of verifying the authenticity of a user's access to a system. If user access is not protected, it can become the first target point of entry for the attacker and impact the confidentiality, integrity, and availability of data to legitimate users. During COVID-19, many people witnessed issues with remote login due to authentication breakdown. Poor authentication can cause many attacks such as man-in-the-middle, distributed denial of service, ransomware, spear phishing etc.

Authorization: Due to COVID-19, many challenges are faced with the authorization of users, such as assigning proper roles and privileges to a verified user.

Accountability: Due to COVID-19, many organizations faced poor accountability as they couldn't keep track of their digital footprint, which ultimately generated trust issues.

Incident Management Challenges

Due to immediate work from home restriction, many organizations lacked the full incident response cycle plan, i.e., identification, containment, eradication, and recovery. Moreover, many organizations cyber incident management teams lacked how the incident needed to be handled at the time of the attack, and it gave rise to unconventional reporting.

Remote Communication Challenges

Due to COVID-19, organizations adopted video conferencing and telecommuting as an alternative for work from home to maintain office productivity. But it also opened the way for attackers to target networks and unsafe systems/applications. During WFH, some organizations have strict policies for remote access, while others did not, which created challenges as listed below:

- Unsafe Networks, unencrypted channels, weak authentication protocols, outdated device drivers, unpatched software.
- Struggle in a change of mindset of employees.
- Many companies were totally unprepared to handle challenges during pandemics.

Healthcare Data Management Challenges

The healthcare industry's data is very critical as it involves private medical details and personal information. Personal information is a basis of trust; therefore, it was very challenging for the

health care industry to maintain integrity. At the same time, the healthcare industry was the core of cybercrimes due to pandemic, and hackers were targeting poorly-protected systems to disrupt the operations and steal sensitive data. In one disturbing case during the COVID-19 pandemic, cybercriminals attacked a hospital and COVID-19 test in the Czech Republic, pressurizing the hospital to shut down in case of urgent surgeries and acute patients. Therefore, ransomware attacks were targeted at hospitals. Many attackers also violated the confidentially and integrity of a person by using social engineering as their entry point.

Technology Defenses during Hybrid Work Environment

The challenging cybersecurity incident during the pandemic required an approach to protect digital assets and offer better performance with minimal disruptions. A defence in depth model control measure ensures that the data/asset is protected with two or more layers of protection for maximum security.

DEFENCE-IN-DEPTH

The scenario of defence in depth is defined as an authentication server that is hosted on a remote virtual machine, protected by three hardware-based firewalls, and hosted inside a biometrically secured data centre. The data centre is secured with environmental control systems and fire management solutions. However, due to covid, there are many countermeasures that companies took to protect from theft:

Technical Countermeasures: It represents the tangible security assets that are used to protect the computer resources or networks against real attacks. It includes software-hardware systems such as antivirus software, encryption software, network monitoring tools etc. In times of pandemic, encryption is an aspect to protect the documents being exchanged between different parties to maintain the integrity and confidentiality of users. While due to covid, all online purchase orders, consent transfers, contracts need to be verified, and for that, *DocuSign* is a tool that enables parties to use electronic signatures for validating contractual agreements remotely.

Control Knobs Countermeasures: Control knobs are safety control measures to protect computer systems and networks from security risks and balance the effectiveness conforming with the defence-in-depth model. For example, in the pandemic, when every organization, school, college institution had to work remotely, it became obvious to use Zoom (an online video telephony company) for work interactions and corporate meetings. Companies used the '*waiting room*' feature of Zoom for optimization. It helps the meeting administrator to carry out a pre-screening

of participants to check if they are valid before enabling them to enter the meeting session. The waiting room functionality helps an organization to minimize the risk of zoom bombing in which the attackers use man-in-the-middle attacks to record meeting conversations or post offensive content that could harm the privacy of a company.

Another preventive control organization used during the pandemic was the installation of an effective anti-malware tool to identify harmful contents to the computer. A good antivirus solution will prevent malicious code from being executed. For maximum efficiency, antivirus software needs to be fully updated by antivirus software providers.

Administrative Countermeasures: Corporate organizations also need to implement technical guidelines by keeping track of behavioural adaptations of digital upsurge by consumers in response to the COVID-19 pandemic. In addressing issues, people falling prey to online scams, the world health organization academy announced a mobile App(available to both Android and iOS) to help people seek the COVID-19 information. The mobile app gathered trustworthy information from different platforms and therefore prevented users from clicking on any fraud website.

Therefore, it was essential for an enterprise to have security deployed with a combination of administrative, control knobs and technical countermeasures.

Secure DevOps Approach to protect Intelligent Systems

With the advent of Intelligent systems, the world has become interconnected. The rise in connectivity has also increased the concerns related to safety and security. Therefore, a higher level of security must be achieved while developing critical systems so that they can remain strong in case of any cyber-attacks, as every organization is looking for an agile, flexible, and cost-efficient solution to improve their workflows. DevOps gained huge acceptance with its faster, better collaboration and communication for testing, software release and team building as developers are always looking for a way to innovate and make products and software faster. On the other hand, operation teams are looking for a stable, reliable system. These two approaches can make this challenging from the security concerns. A common practice in the DevOps model is continuous integration and delivery. It is also characterized by its 'speed,' to deliver products on time and 'reliability,' to make an application less error-prone.[76]

Need for Integrating DevOps in Security

An Internet of Things (IoT) system includes gateways, client devices, backend cloud, databases, storage systems, end-user applications. The setup of the IoT system is distributed in nature rather than centralized. Therefore monitoring, diagnosing and analyzing these systems are more challenging. From the security point of view, whenever a new system is created, organizations need to think of security from the start. In many companies, security is considered as a non-functional requirement as it doesn't come in the functionality, but if a system is not tested from the start, security at the end can move the deadline of the project, costing a lot of time and resources. This can create inefficiency in the process. Therefore, architects moved the process of security from the end to be distributed throughout the pipeline (as shown in figure 45). [77]

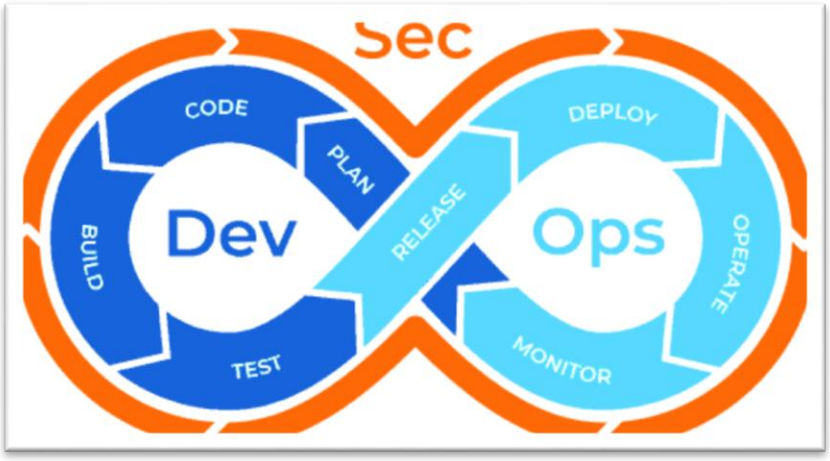

Figure 45: DevSecOps Cycle [77]

DevSecOps

DevSecOps is a combination of security, development, and operations [78]. A DevSecOps framework ensures that security is built into applications at every stage of the Software Development Life Cycle. It makes the team conduct application security by executing security measures at the same step as development and other operations tasks. An organization implementing DevOps is shifting towards a DevSecOps technique to achieve higher excellence in security, therefore, minimizing vulnerabilities. Some major benefits of DevSecOps are it provides automation from the start of a process to reduce the chances of any vulnerabilities. Also, it reduces the load on security engineers to manually construct security supports. Below mentioned are a few benefits of Secure DevOps:

- DevSecOps reduces cost.
- The effect of DevSecOps goes beyond an individual system's development.
- Secure DevOps is an agile process.
- Increases the overall quality of products, processes, and services.
- Speeds up continuous deployment
- DevSecOps combines the whole system's lifecycle.

Impact of Secure DevOps on Enterprise

Implementing secure DevOps produces results that go beyond the company's internal assets to strengthen its market position, increase innovation, and create new business opportunities. Security in DevOps helps companies to strengthen their reputation in the technological sector. Adding

security by design in the development of system architecture enables companies to grow their client base, target new customers and be unique in the IT market.

Secure DevOps Approach [78]

Figure 46 illustrates the secure DevOps approach to construct and update new product development (including people, organization, business, infrastructure, and process) in real industrial companies. It supports the following features:

- Continuous identification of business requirements.
- Continuous monitoring of evolving cybersecurity threats.
- Synchronizing the collaboration between DevOps and the security workforce with other stakeholders.

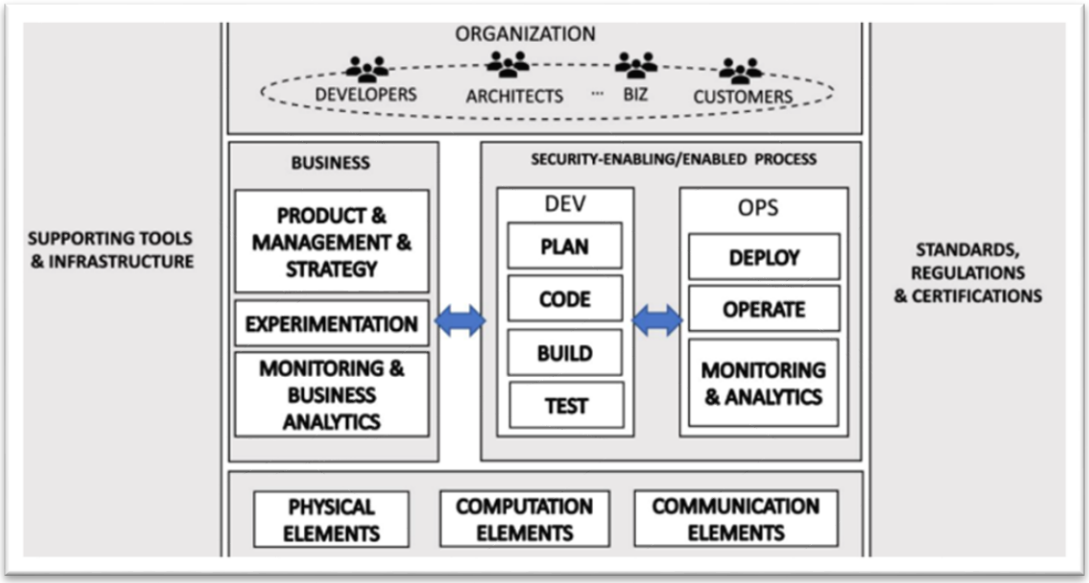

Figure 46: Developing, shipping, and operating competitive Cyber Physical Systems in a secure manner with DevOps [78]

Case Studies

In an enterprise, security teams alone cannot avoid the security incidents and therefore the first step of any organisation should be to implement continuous security tools. The goal of any DevSecOps strategy should be, how to make organisation's data resilient to attacks and protect most valuable data/products. Below mentioned are some case studies from different enterprises, to determine that effect where implementation of a DevSecOps have proven to be a success [79]:

U.S. Air Force

Nicolas M.Chaillan, former Chief Software Officer of the U.S. Air Force, implemented DevSecOps approach to solve the jet's legacy hardware challenge. The challenge was to boot Kubernetes with Istio (control plane) on the jet within two minutes if something goes wrong. Moreover for U.S. air force DevSecOps has been a big game changer as previously most military software teams were using waterfall model and the software delivery would take three to ten years. The Defense Department took a new approach to DevSecOps, that used Kubernetes clusters and other open source-technologies to speed up their releases. Releases, which were previously taking three to eight months now can be attained in one week.

HSBC

HSBC bank operates across 64 countries and wants to remain a sustainable data driven organisation by not only giving fast responses to customers but also placing a robust technology model to predict what customers want. HSBC Americas, EVP and CIO, Donald Patra, said that usually the projects need to deliver in 12 weeks, that set security challenges especially when organisation is using IaaS (Internet-as-a-Service) and PaaS (Platform-as-a-Service) services. Moreover, if the security services are left for last week, there is not enough time for fixes, verifications, and reviews. To solve this challenge, HSBC paired a software developer with security skills at every step to become more cross-functional and engaging across teams.

Cybersecurity service providers

Symantec

Introduction

Symantec Managed Security services is a comprehensive threat detection service that provides 24*7 security monitoring that is needed for prioritizing and responding to critical incidents. Moreover, it builds strategies that are required to protect the organization's assets and address business goals. Symantec has a designated team of service managers, principal analysts, incident handlers, engineers that learns about the organization's environment, network, business goals, processes and focuses on detecting and responding to cyber threats. The purpose of Symantec's global team of experts is to make sure that the organization understands the threat patterns, address security gaps and strengthen their security profile.

Symantec's MSS Analytics Engine

Symantec's Global Intelligence Network is the world's largest civilian threat intelligence database which complies with real-work enterprise and consumer data from Symantec's extensive network (using endpoint sensors). Then Symantec correlates that data with organization logs to identify any signs of compromise. Symantec's security operations center technology platform process 160+ billions of logs each day, inspecting any patterns of malicious activity [80]. Therefore, Symantec's GIN provides the deepest level of visibility across endpoint, email, web and cloud traffic to detect and block targeted attacks. Figure 47 represents how MSS analytics detect the threats.

Figure 47: Detect the unknown with MSS Analytics [80]

Symantec's Integrated Cyber Defense

The Symantec Integrated Cyber Defense is a comprehensive threat protection compliance that delivers endpoint security, network security, information security and identity security on cloud and on-premises infrastructure, as shown in Figure 48.

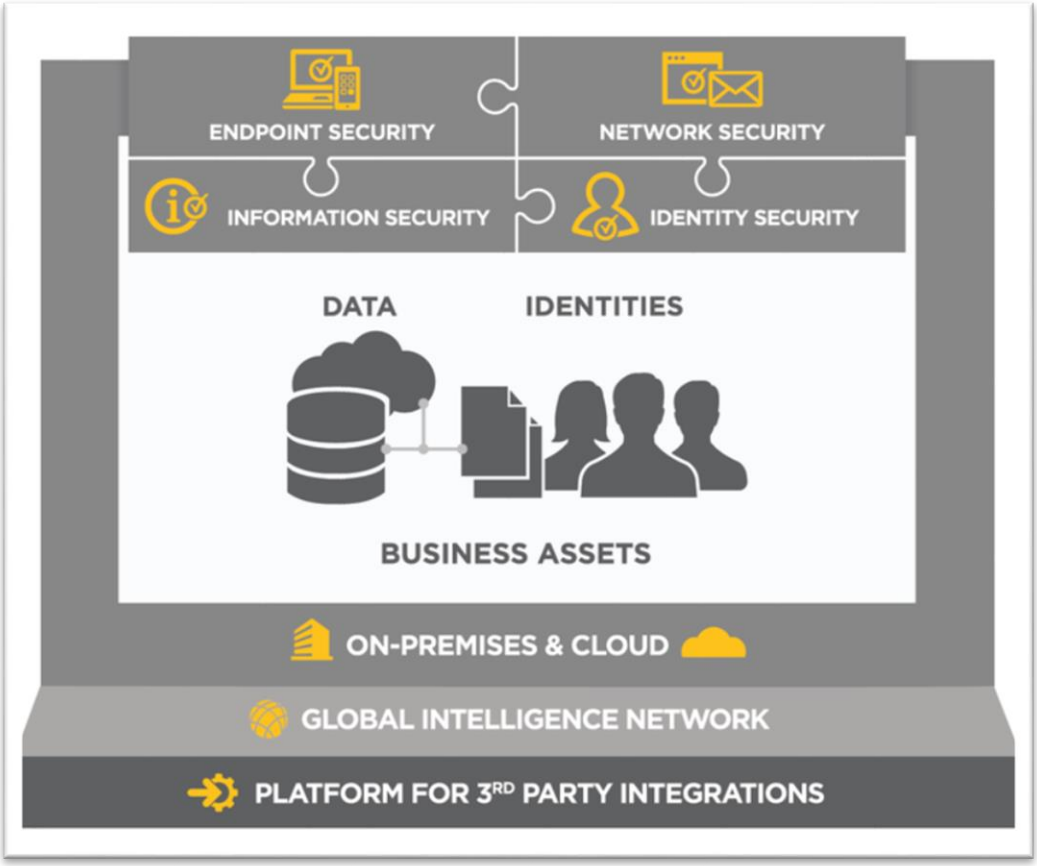

Figure 48: Critical Security Solutions – Integrated [81]

An integrated solution is an excellent approach that reduces operational complexity and protects assets data in the industry. It unifies products, services and partners to reduce the cost and complexity of cybersecurity threats [81]. It combines all the benefits with global intelligence and automation across networks, applications, endpoints and clouds. Below listed are a detailed explanation of ICD components:

1. Endpoint Security: This defence protects from cyber-attacks by keeping the sensitive information safe on stored devices/data-center(laptops, desktops, mobile phones, servers, cloud workloads) so that they cannot fall into the wrong hands.
2. Network Security: This defence protects the email and web access that are essential for communication. This includes secure web gateway, encrypted traffic management, web isolation.

3. Information Security: This defence protects sensitive documents and information by using a highly integrated set of data protection and cloud security solutions. This includes secure access cloud, data loss prevention and cloud access security broker.
4. Identity Security: This defence protects users and applications so that only trusted users can access applications. This includes identity and access management authentication.

As we know, many organizations are moving to on-cloud rapidly; Symantec is the only cybersecurity service that supports all infrastructure, whether on-premises, hybrid or cloud. Moreover, as we know that Symantec will never be the only vendor; therefore, their solution (integrated cyber defence Exchange) in which third-party products can be combined and can share intelligence across the platform.

Akamai

Keeping the users and websites safe from online threats requires deep expertise in proactive monitoring and a fast incident response plan in a single managed service. Akamai's Managed security services help the organization to achieve a strong security posture to protect from defences [82]. Through services like early detection of an attack or providing actionable insights about the attack, an organization can respond to mitigate against threats. MSS regular updates security design helps to keep updated with the highest level of protection. MSS maps a security strategy using Akamai Intelligent edge platform to integrate best practices for an organization according to business needs. MSS also supports Akamai cloud security solutions to prevent harmful DDOS attacks, bot attacks etc.

Akamai Managed Security Service

Figure 49 represents how Akamai's managed security services work:

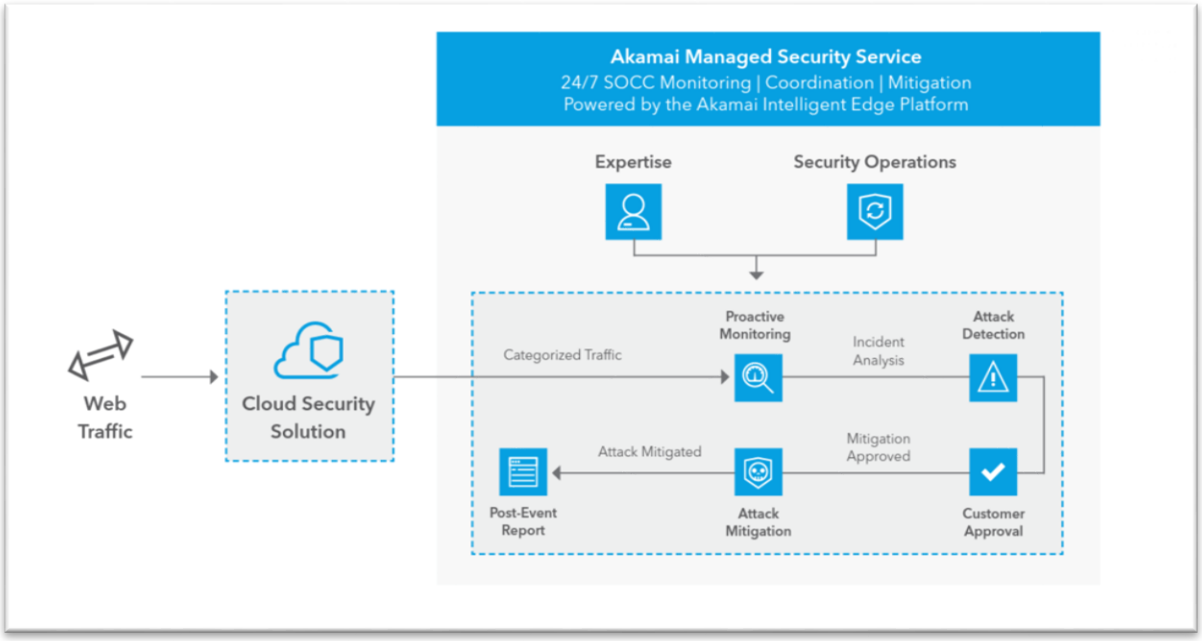

Figure 49: Akamai Managed Security Service [82]

Here are some key features mentioned:

Proactive Monitoring: This feature is essential to provide early threat detection. Security experts provide 24*7 real-time monitoring and analysis to detect anomalies and protect against possible threats.

Security Event Management: After a threat is identified, security experts do a deep analysis highlighting the attack behaviour and then list the possible actions. Security experts have to maintain the SLA's also by responding to any incident as fast depending on the severity level.

Attack Readiness: Security experts need to optimize the Akamai security configurations periodically with tuning recommendations to protect against the latest threats.

Advisory services: In this, a security expert will provide the summary of security activity, security posture, and Security recommendations to maintain the business priorities.

Cybersecurity Risk Management

Introduction

In every organization, cyber risk calls for serious attention. The most important understanding for an enterprise is to accept the reality of the risk and not hide or deny it. For example, in 2016, uber faced a data breach affecting 57 million customers as the administration concealed the breach for more than one year. If Uber's administration had followed the incident response plan, the impact would have been much less. Therefore, organizations must understand what factors can cause risk, and leaders must consider focusing on and identifying the cyber risk targets. Cyber risk can cause the loss of Confidentiality, Integrity and Availability, which causes fraud, business risk, financial crime, and unavailability of the system. The main objective of risk management is to maximize the probability of positive events and to minimize the probability of bad events. To safeguard the CIA of an organization, a risk assessment is performed, which is an essential part of an information security audit. For accessing the information security risks, either qualitative or quantitative methodologies are used.

What is a Risk?

All organizations face some kinds of risks. Risk is the probability that a loss will occur, and losses occur when a threat is exposed to vulnerability. Some enterprises face a severe risk that causes their businesses to fail, while some risks are minor. Companies use risk management techniques to identify the risks and then decide whether to avoid, share or transfer, mitigate, or accept the risk. In the case of an IT enterprise, the major components of risks are:

- *User Domain risks:* These risks are caused by users, employees, contractors, or consultants of an organization. For example, an employee visits a site and download infected software. This can infect other computers and the entire network.
- *Workstation Domain risks:* These risks are caused by the end user's computer. If the antivirus software or any patch is not updated, it can harm the organization with malware.
- *LAN Domain risks:* Network devices such as switches, hubs and routers are connected together on the local area network. If each network device is not protected, attackers can use sniffing attacks to capture data packets and can become a major cause of risks for an enterprise.

- *Remote access Domain risks:* Most employees in an organization need remote access while connecting to the organization's network. Remote access is granted via a virtual private network. Since the internet is usually untrusted, attackers can use unprotected connections to enter into remote servers and cause risks for an organization.[83]

The Risk Management Process

Cybersecurity risk can cause harm an organization's reputation, assets, and information systems (loss to CIA trait). The main intention of the cybersecurity risk management program is to make sure that risk issues are combined into the strategic decision-making process to achieve the performance goals. The common process for managing cybersecurity risk in an enterprise is illustrated in figure 50. [84]

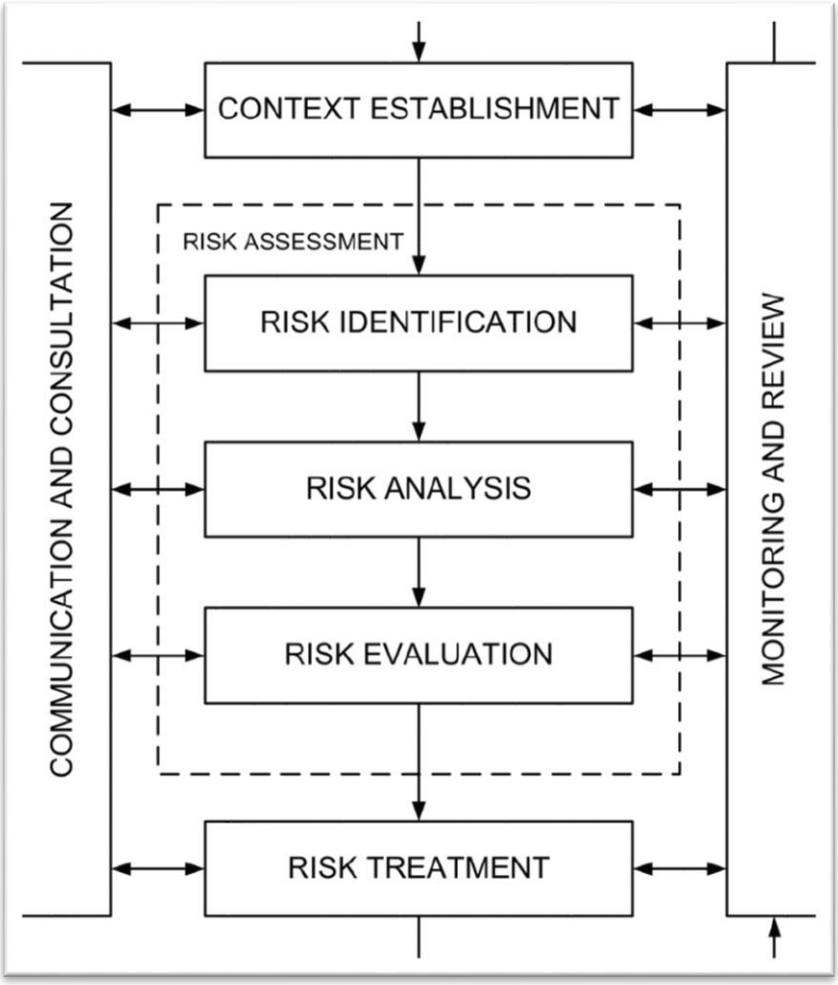

Figure 50: The overall risk management process [84]

Context Establishment

The first stage of the risk management process is to understand the context in which an enterprise operates so that all the factors should be considered according to the context.

Risk Assessment

The risk assessment process is broken down into three areas: Risk identification, risk analysis and risk evaluation.

Risk identification [85] is a process of discovering, defining, describing, documenting, and communicating risks before they become the problem. This process is most crucial as it is important to ensure that a wide range of risks are identified, because the risks excluded at this step may not be handled in successive steps. Not only the risk management experts are responsible for identifying the risks, but project managers, project team members, stakeholders, end-users, customers are all responsible for identifying the risks. After the identification, all the risks are entered into a 'Risk List'. A risk identification may further proceed into 'quantitative risk analysis' and 'qualitative risk analysis'. The starting point of risk identification is to gather all the valid inputs that a project manager and the team will need to understand the outcome of risks. The inputs are defined below:

- *Enterprise Environmental Factors:* These factors include all external and internal environmental factors that may affect the projects. These include market conditions, the company's culture, infrastructure, legal restrictions, government regulations, existing resources, project management software, commercial databases, academic and industry studies that are useful in identifying risks.
- *The Project Management Plan:* The project management plan is useful in gathering all the critical information like the project's mission, Work Breakdown Structure (WBS), scope, schedule, cost, quality criteria to review all the possible risks.
- *The Risk Management Plan :* Assignment of Roles and Responsibilities, Budget provisions for Risk Management Activities, Schedule for Risk Management, Categories of Risk.
- *Organizational Project Assets:* Organisational project assets provide previous information, historical information and lessons learned.

- *Project Scope:* The project scope statement is the first step in the project and should be clear to everyone. However, if there is an assumption or uncertainty in the project's scope, it should be considered as valid input in identifying the Risk.

Cybersecurity risk occurs when a threat is exposed to vulnerability. Therefore, to identify risks, we need to identify the threats and vulnerabilities and then evaluate the odds of happening that vulnerability. When assessing the threats, many enterprises use a model known as 'D.R.E.A.D,' which asks five questions [84]:

Damage: How bad an attack be?

Reproducibility: How easy is it to reproduce the attack?

Exploitability: How much work is required to initiate the attack?

Affected users: How many users will be impacted?

Discoverability: How simple is it to discover the attack?

The answer to each of these questions is allocated by assigning various attributes to Risk, like impact, description, time frame and probability, as shown in Tables 1 and 2.[91]

Table 1 shows the impact and description.

Impact	**Description**
Critical	If this occurs, the program will fail as the minimum requirements are not met.
Serious	If this occurs, minimum requirements are met but not secondary requirements; and will increase the major cost and schedule.
Moderate	If this risk occurs, minimum requirements are met, but some secondary requirements are not met and will cause some minor increases in budget cost and schedule.
Minor	If this risk occurs, the minimum requirement is met. Also, some secondary requirements are also met but will cause some small increases in budget cost and schedule.

Negligible	If this risk occurs, it will have no effect. All requirements will be met.

Table 2 shows the probability and description.

Probability (in %)	**Description**
0-20	Very unlikely the risk will occur
21-40	Unlikely the risk will occur
41-60	Even likelihood the risk will occur
61-85	Likely the risk will occur
86-100	Very likely, the risk will occur

Risk analysis

Once the initial risk identification is conducted, the organization will take the impact and probability of risk and combine them in a risk matrix, as shown in figure 51.

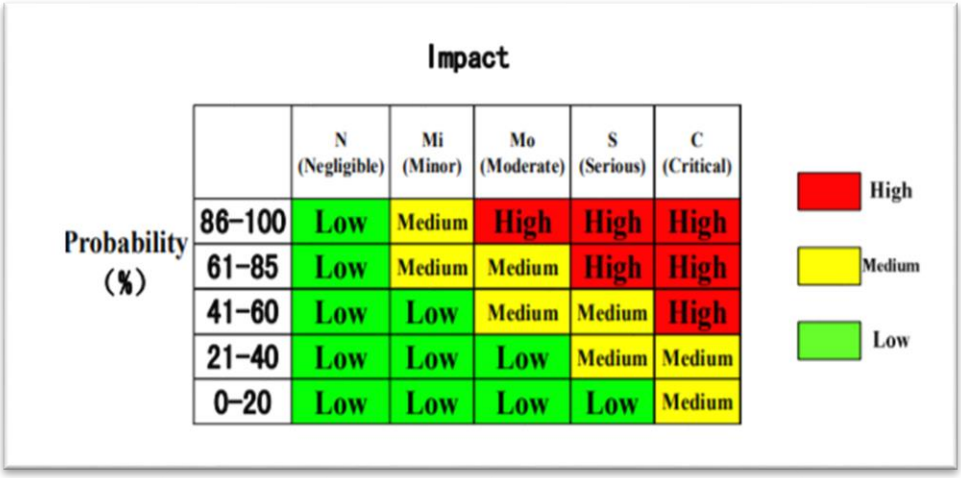

Figure 51: Risk matrix [91]

The risk matrix is a pictorial representation of corresponding levels of all the identified risks. This allows an enterprise to understand and prioritize how to treat them. Below table shows a description of risk handling options [91]:

OPTION	DESCRIPTION
Terminate (Avoid)	Terminating risk is of the most feasible approach which involves eliminating the risk.
Tolerate (Accept)	Tolerate a risk is to accept a risk because the cost of mitigate or reduce a risk is very high. However, these risks should be monitored because future changes may not make it tolerable.
Transfer	Some risks are best treatable by transferring them to a third party who are ready to take the risks.
Treat (Reduce)	Treating a risk is to do take some measures to reduce the impact of risk like installing a firewall will reduce the likelihood of an external intrusion to your IT systems.

Risk Evaluation [84]

After analysis of risks, there are four ways in which an organization can deal or treat risks, as shown in the figure 52:

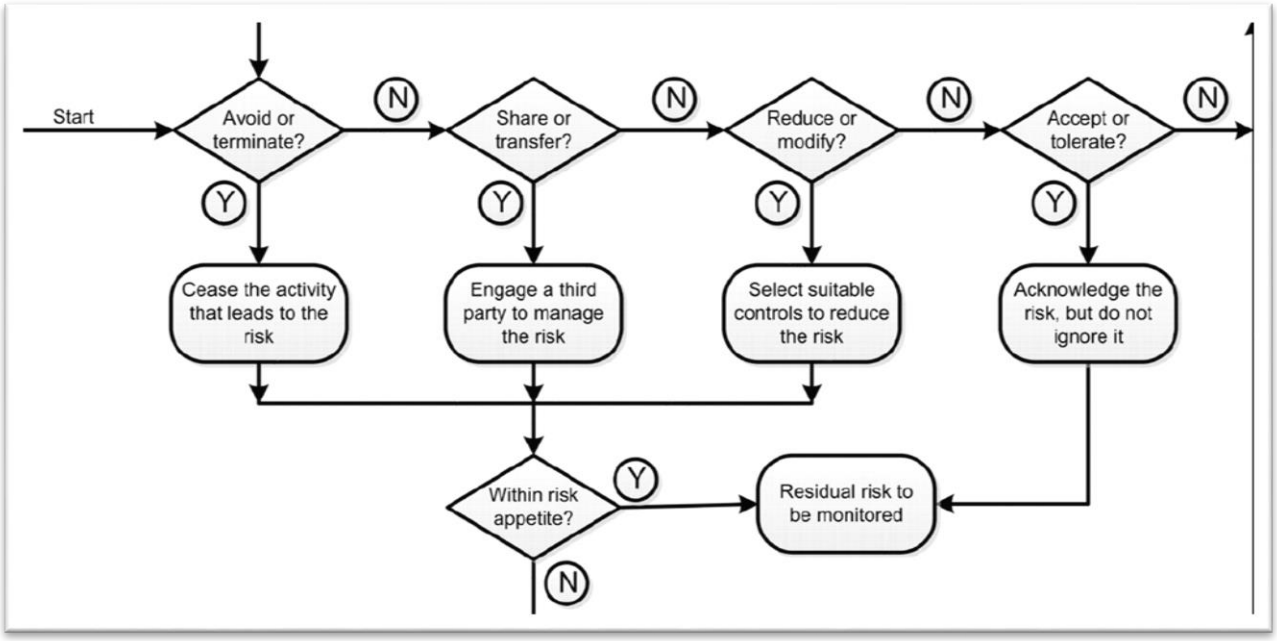

Figure 52: Strategic risk management options [84]

Risk avoidance or termination [83]

In this method, the organization either stops doing whatever is accusing the risk or avoids doing it. For example, if an organization is building a data centre and after risk assessment, it is indicated that there is a high likelihood of flooding in the preferred location. To avoid the risk, the organization decides to abandon the location and start building a data centre somewhere else. However, there are some problems with this decision like the new site can be difficult to locate or it might be costly. This helps the organization in reviewing all these risks against one another.

Risk Sharing or Transfer

Organizations can share transfer risk by shifting entire responsibility to third-party insurance companies.

Risk reduction [83]

This is also known as risk mitigation. In this, organizations can reduce risk by reducing vulnerabilities and implementing some countermeasures or controls. However, the cost of a control

should not exceed the benefit. Below are some examples of mitigation steps taken by the organization:

- Implement a backup plan if any system goes down.
- Teach technical staff on social engineering tactics.
- Implement intrusion detection and intrusion prevention systems. Also, keep the antivirus software up-to-date.
- Replace hubs with switches to prevent traffic overloading.

Risk acceptance [83]

Risk acceptance shows the organization's attitude towards risk. For example, if an IT organization is hosting a web server for any e-commerce. The web server is generating $2000 per month in revenue (Revenue per hour will be: $2000*12/365/24=$2.7). The organization first decides to host a failover cluster if the web server goes down and it costs approximately $20,000. On the other hand, if a server goes down for 1-2 hours, the loss will be less than $3. Therefore, in this case, the impact or likelihood of risk is very low, and the final option for an organization is to accept the risk.

Residual Risk [84]

While performing the risk treatment, some risks are completely removed while some number of risks are left and called 'residual risk.' These risks are too expensive, or it's not possible to treat them. These risks must be accepted by an enterprise and require continuous monitoring and regular reviews to ensure that it doesn't grow.

Risk Treatment

Risk treatment is also known as risk mitigation, which is taken to reduce the impact or likelihood of risk and its occurrence. It combines the use of different controls or countermeasures to carry out risk mitigation [84]. Below defined are four distinct types of controls:

- Preventative controls: stops something from happening.

- Directive controls: refer to some form of procedure that must be followed.
- Corrective Controls: used to fix a problem after it has occurred.
- Detective controls: aware us when something is actually happening or has happened.

Detective and corrective controls are taken once an attack has actually happened. However, directive, and preventative controls are carried out before an attack has happened to reduce the impact. These four controls are implemented in one of the three ways defined below:

- Physical Controls: These controls are taken place to prevent any harmful physical activity, such as fitting locks on computer room to block unauthorized access.
- Technical Controls: These controls are taken place to change the way in which software or hardware operates, such as implementing firewalls rules in a network.
- Procedural Controls: These controls are taken by an organization to provide immediate actions taken by employees in any particular situation, such as the requirement to change their passwords after every 15 days.

PDCA (plan-do-check-act)

Organizations are also following the PDCA model for continuous improvement in business processes [84]. The PDCA model is, also known as the Deming circle, implemented by enterprises to improve the quality and efficiency of the risk management framework. The PDCA cycle is illustrated in figure 53, and the four stages are described below:

Plan: In the cybersecurity context, this stage equates to understanding the organization and its context.

Do: This stage determines the implementation of the cybersecurity risk management framework.

Check: In this stage, the results of the implementation are tested, monitored, and reviewed.

Act: In the final stage, the validated plans taken by organizations are put into action when an incident occurs. These actions guide the lessons learnt from previous incidents and bring revisions to the plan.

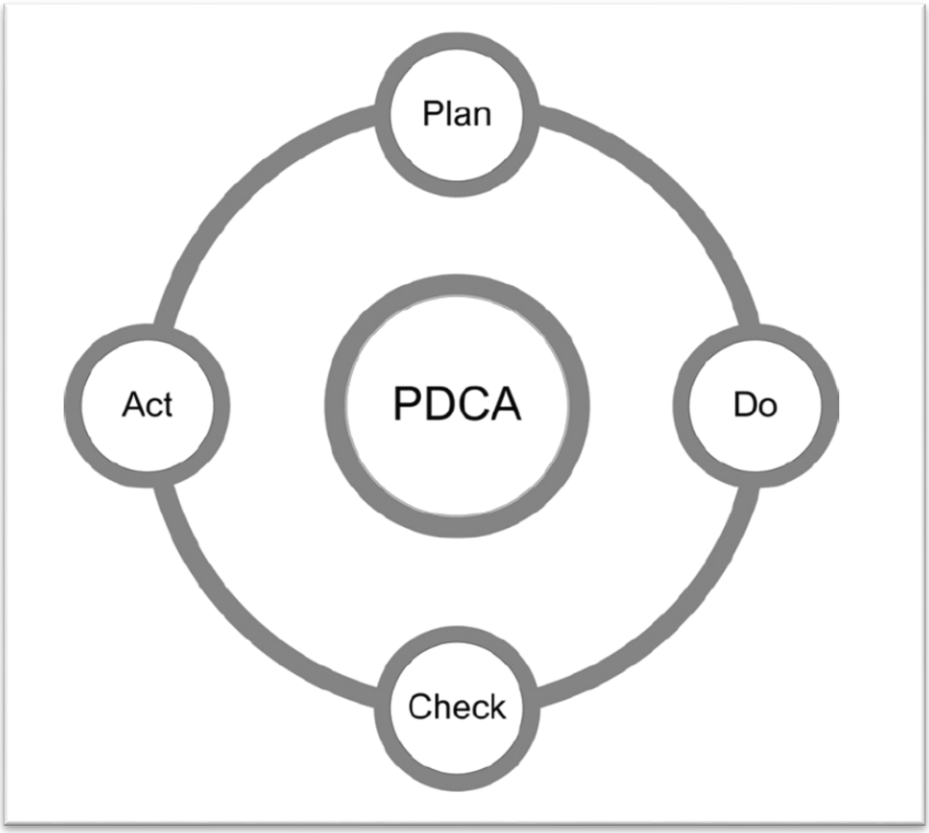

Figure 53: The Plan–Do–Check–Act cycle [84]

NIST 800-39: Risk Management Process

NIST 800-39 SP provides a flexible structural approach of managing, assessing, responding, and monitoring risks to a diverse group of risk management professionals, including CEO, Business owners, Senior Information security Officers, Program Managers, Security Engineers, systems evaluators etc. Risk Management is a complex process and requires organizations to use an effective continuous loop to address risk [86]. Figure 54 illustrates the four components of the risk management process. The bidirectional arrows represent the flexible communication flow.

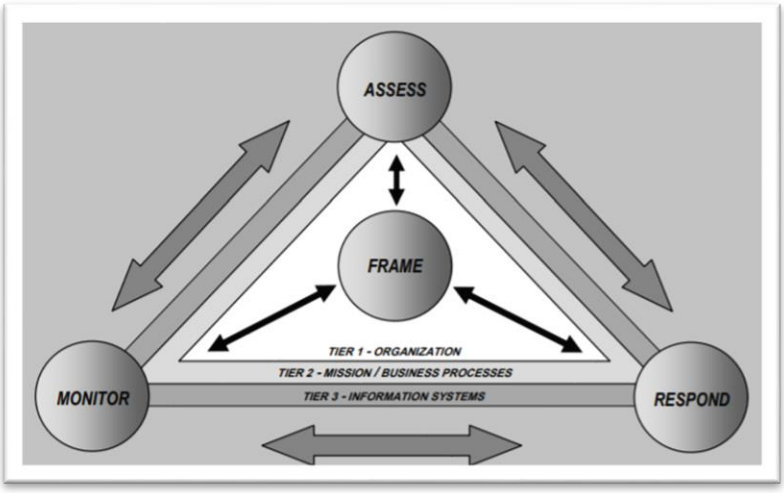

Figure 54: Risk Management process applied across the tiers [86]

Frame Risk

The first component describes an environment in which risk-based decisions are made. After this, a risk management strategy is defined that will make how the organization will assess, responds, and monitor risk. A risk frame is the main base for managing risk by identifying:

- *Risk assumptions:* Assumptions made about threats, vulnerabilities, impact, the likelihood of occurrence that reflect how risk is assessed, responded to and monitored over time.
- *Risk Constraints:* Issues in an organization that slow how risk is assessed, responded to and monitored.
- *Risk Tolerance*: There are some components like levels of risk, degree of risk, types of risk that define how risk is handled.
- *Priorities and Trade-Off:* Trades-off among different types of business functions, time frame in which the risks are addressed and relative priority of any mission.

At Tier1, executives or senior leaders define the organizational risk frame, how risk is assessed and how risk is monitored. At Tier2, business owners define the organization's risk frame by addressing constraints, priorities, and assumptions. At Tier 3, Program managers and system owners define risk frames on the basis of Tier1 and Tier2 decisions.

Assess Risk

The second component describes how organizations assess risks. There are many ways to identify:

- Analyze the possible threats (or hazards) to an organization directly or through a different organization.

- Identify the vulnerabilities external and internal to the organizations.
- Analyze the harm and its likelihood that would occur when vulnerabilities are exploited against possible threats.
- Decide what tools, technologies and methodologies are an organization uses to assess the risk.
- Identify how to meet the legal requirements of a business.
- Provide an analysis of various sources and methods to obtain the threat information.
- Assume what can be harmed and how.

A risk assessment conducted at different tiers will have a different objective. In Tier1, risk assessment can be based on assumptions, priorities and trade-offs, constraints. Before entering the risk response step, an organization-wide risk assessment is a prior decision for decision-makers.

Respond To Risk

The third component describes how to respond to risk based on loss and impact after it has occurred. Specific actions should be taken based on the agreed risk tolerance strategies. Risk Response includes avoiding, accepting, mitigating, and transferring risk. In addition, organizations also identify various methodologies for responding to risk and communicate appropriate communication to external service providers. Risk decisions can be executed at any of the tiers with different objectives. For example, at Tier1, risk response decisions are made organization-wide. Business process supporting resource requirements are implemented at Tier2. At Tier3, action is defined in terms of the maximum amount of time to implement the selected action in terms of SDLC lifecycle.

Monitor Risk

The fourth component in risk assessment is to monitor the risks. This can be achieved by studying the risks and seeing how they will impact the Key risk Indicators (KRIs). Below are some functions of risk monitoring:

- Verify that risk response compliances are implemented, and all the requirements are satisfied.
- Check the effectiveness of risk response measures.
- Check the internal audit reports to evaluate whether a business is performing correctly by taking agreed-upon actions.
- Determine the impact of changes to an organization's information system.

- The organization will have a clear picture of whether they need to revisit other steps in risk management.
- Maintaining the awareness of risk being induced.

Tier1 monitoring activities include how changes in threat assessment may affect Tier2 and Tier3 activities.Tier2 monitoring activities include analysis of technologies to check the weaknesses in those technologies that may affect the business. Tier 3 monitoring activities include vulnerability scanning and monitoring of security controls for all the information systems.

NIST 800-37: Cybersecurity Risk Management Framework

NIST SP 800-37 focuses on active monitoring of the system using the SDLC lifecycle [87]. The CRMF labels the nature and scope of threats in real and provides a number of benefits to achieve the flexibility in security lifecycle:

- Conveying the key functions of security programs like governance, compliance, risk, management, operations.
- Assessing key vulnerability points of cybersecurity: people, processes, and technology.
- Interpreting the state and maturity of a cybersecurity program.
- Continually assessing the enterprise risk posture.
- Maintain the awareness of cybersecurity posture in the organization.

The CRMF emphasizes three principles:

- Applying best practices to secure the information system by blending information security into the system development lifecycle.
- Achieve situational awareness by reporting processes, monitoring and maintaining information systems using both manual and automated mode.
- Accepting risk and its impact on assets, individuals, and organizations.

The objective of CRMF is not to put all the pressure on senior levels but to establish clear business processes appropriate decisions to permit the flow of risk information at relevant levels as Cybersecurity risk management cannot be beneficial in silos. To certify that risk information is extending out to appropriate clients, enterprises must implement an agile model employing ERM. This model will help in maintaining transparency in decisions and securing the business processes.

Risk-Based Standard [88]*:* Risk analysis includes risk assessment, management, and communication. In a large-scale system, the risk is defined as the particular of what can go wrong, the likelihood of that event will occur, and the consequences, i.e., threat*vulnerability*consequence. Risk assessment quantifies the risk posed on each system component. The goal of the quantitative analysis is to identify the contribution of each module and check which component is the risk-based standard. Nowadays, the traditional risk analysis approach is not enough to cope with cybersecurity complexity and dynamics. On October 22, 2013, NIST released a document on a risk assessment framework that guides to choose actionable mitigation strategies instead of the traditional approach.

Risk Assessment in IoT Systems

As there are many methods to assess risks but the increase in technology, automation and complexity of IoT systems will increase challenges to solve the new risks. Therefore, there is a need for new methods that will assess the risks while considering the uniqueness and dynamics of the IoT systems [89]. The main challenge is that all the traditional methods to assess risks were developed before the IoT systems were established. Below mentioned are some current risk assessment concepts:

- Risk Assessment is the process of identifying, estimating and prioritizing risks according to organizational assets and operations. It involves various options like *Risk Acceptance* if risk cannot be mitigated. *Risk Mitigation*, to treat the risk using security controls; *Risk Transfer*, if risk can be transferred to a third cyber insurance party; *Risk Avoidance*, risk can be treated by removing the affected assets. For assessing the risk, the main core concepts are to understand a company's assets, vulnerabilities, threats, the likelihood of the attack and the impact of a cyberattack.

Assets of an organization can be tangible(infrastructure) or intangible (business process, reputation). Vulnerabilities are the weaknesses in the assets. When a vulnerability is exposed, a threat results, which can adversely affect the business. Cyber risk is harm caused to an organization due to the probability of a successful threat or attack.

- There are various approaches for risk assessment from standard bodies such as NIST, ISO/IEC and CRAMM (from the UK), which are applied in enterprises to assess risk. Some of the most popular include NIST SP800-30, ISO/IEC 27001, CCTA, Risk Analysis and Management Method (CRAMM) and Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE).

Figure 55 represents the IoT components and their main advantage that it can expand as the new system grows. Also, the components of IoT systems are loosely coupled, i.e., once the task is completed, the connection can be broken down. As the behaviour of the IoT system is spontaneous or temporary, it is challenging to track the behaviour or devices from a security point of view.

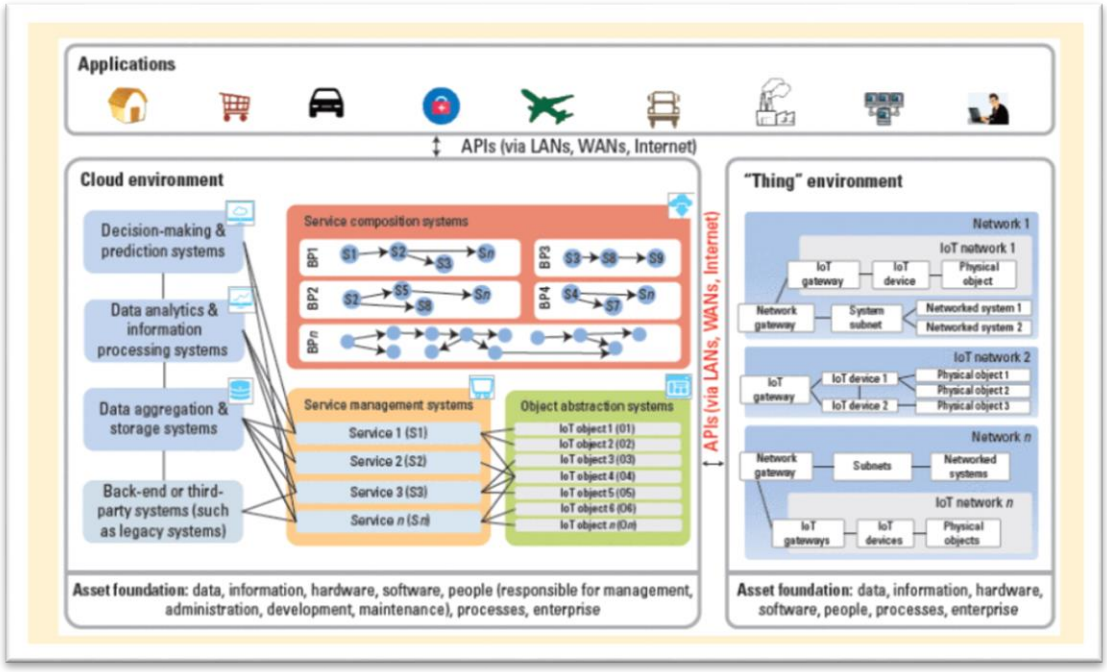

Figure 55: Components commonly featured in internet of things systems [89]

Shortcomings of Current Risk Assessment

Below discussed are some key points that must be controlled to bind the trust in an IoT environment taking in mind the dynamics and challenges of an IoT system:

- Current Risk Assessment techniques are based where systems will not change in a short period of time. However, this assumption does not hold for IoT systems where the components are loosely coupled.
- In IoT systems, limited system knowledge is acquired, which in turn could result in not getting proper knowledge of risks.

- In IoT, devices can be considered as the basis of attack, whereas in the current risk assessment, assets are considered to be protected, not as possible attack platforms.

Therefore, there is a need for automated and continuous risk assessment approaches to support IoT dynamics.

Mitigating Risks and Vulnerabilities

Cyber insurance [90]

Nowadays, many companies are buying a cost-saving cyber insurance approach to achieve a proper balance between acceptable loss and security investments, because to protect a business fully is not economically feasible. Below figure shows the risk management strategies that businesses are using to protect all systems fully.

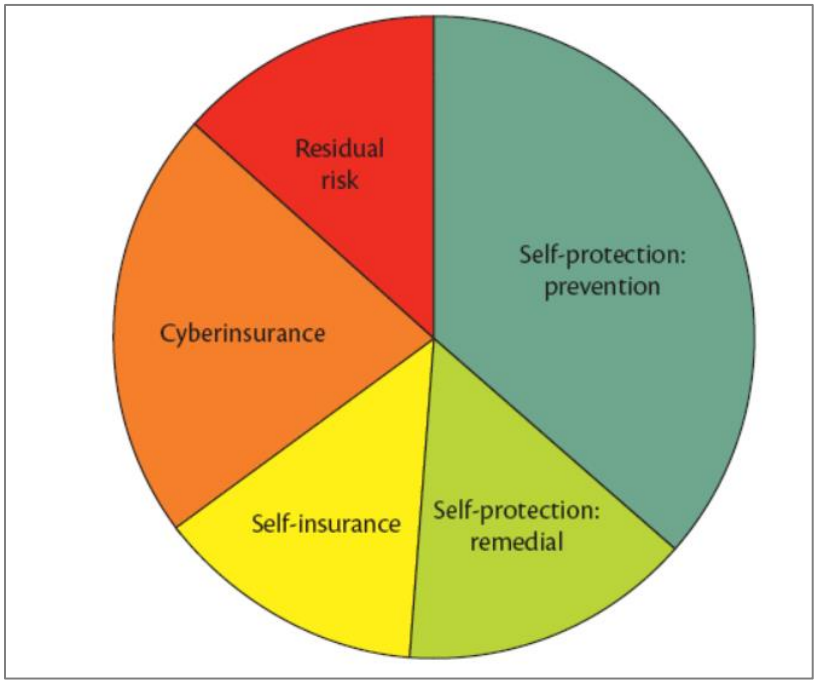

Figure 56: Risk-management strategies [90]

Cyber insurance is the transfer of financial risk to a third party for covering insurances due to liability issues, property loss, theft, data damage, computer failures, website defacement or loss of income from a network outage. As larger businesses generally have larger resources (internally or externally), metrics to calculate the loss of data are highly uncertain. However, there is a glitch because cybersecurity is a new domain in the insurance business, and insurers don't know what to

expect from customers due to which there are breaches that are reported. However, most large and medium enterprises are the customers of the cyber insurance market.

Cyber insurance is the transfer of financial risk to a third party for covering insurances due to liability issues, property loss, theft, data damage, computer failures, website defacement or loss of income from a network outage. As larger businesses generally have larger resources (internally or externally), metrics to calculate the loss of data are highly uncertain.

There are many other risk mitigation strategies:

- Keep the software up to date.
- Restricted access
- Disaster Recovery Plan
- Get rid of unwanted hardware.
- Ensure Signed Software Policies
- Stay away from single-factor authentication.
- Search and look for Intrusions in the network.

Conclusion

In this report, a comprehensive analysis of various cybersecurity domains is studied concerning enterprises. Computer security is a broad topic, and with challenging technologies emerging every day, enterprises need to secure their infrastructure with the new platforms and intelligence systems. There is no perfect solution to cybersecurity, but the aim should be to protect every device participating in network communication. Organizations need to implement security as a dynamic process, i.e., security architects should implement and evaluate systems with security controls right from the beginning. Moreover, while designing any new system, security should be a desirable feature like any other desirable features such as being efficient, accurate and user friendly. It should not just be an add-on for later purposes. Enterprises should also use good software engineering practices while implementing a security system. There should never be any unplanned change, as most breaches result from vulnerabilities introduced when making spontaneous changes. Therefore, a change should always be planned. Security testing is another area where enterprises need to pay more attention. Enterprises should also focus on the maintenance of the system for security purposes, i.e., execution of automatic tools for updates and patch management. Lastly, security training is essential for every employee in an organization.

References

[1]M. Tomšů, "Cybersecurity as a New Type of Security and Its New Perception," 2021 International Conference on Military Technologies (ICMT), 2021, pp. 1-7, doi: 10.1109/ICMT52455.2021.9502751.

[2]Auger, G., Scott, J., Helmus, J., Nguyen, K., & Adams, H. (2021). Cybersecurity Career Master Plan: Proven techniques and effective tips to help you advance in your cybersecurity career. Packt Publishing.

[3]E. B. Talbot, D. Frincke and M. Bishop, "Demythifying Cybersecurity," in IEEE Security & Privacy, vol. 8, no. 3, pp. 56-59, May-June 2010, doi: 10.1109/MSP.2010.95.

[4]L. Piètre-Cambacédès, M. Tritschler and G. N. Ericsson, "Cybersecurity Myths on Power Control Systems: 21 Misconceptions and False Beliefs," in IEEE Transactions on Power Delivery, vol. 26, no. 1, pp. 161-172, Jan. 2011, doi: 10.1109/TPWRD.2010.2061872.

[5]P.s, S., S, N., & M, S. (2018). Overview of cyber security. Nternational Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125–128. https://doi.org/10.17148/ijarcce.2018.71127

[6]Canada's Internet Factbook 2021. (n.d.). Canadian Internet Registration Authority (CIRA). Retrieved February 22, 2022, from https://www.cira.ca/resources/factbook/canadas-internet-factbook-2021

[7]Government of Canada, Statistics Canada. (2021, June 22). Canadian Internet use survey, 2020. Statcan.Gc.Ca. https://www150.statcan.gc.ca/n1/daily-quotidien/210622/dq210622b-eng.htm

[8]D. Puthal, S. P. Mohanty, P. Nanda and U. Choppali, "Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions]," in IEEE Consumer Electronics Magazine, vol. 6, no. 4, pp. 24-27, Oct. 2017, doi: 10.1109/MCE.2017.2714744.

[9]What are the 7 layers of security? A cybersecurity report | mindsight. (2020). https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security/

[10]Asset Management. (n.d.). Cisa.Gov. Retrieved February 22, 2022, from https://www.cisa.gov/uscert/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-AM.pdf

[11]Duane C. Wilson, "4 CYBERSECURITY IN LAYERS," in Cybersecurity , MIT Press, 2021, pp.47-66.

[12]What is endpoint security? (n.d.). Mcafee.Com. Retrieved February 22, 2022, from https://www.mcafee.com/enterprise/en-ca/security-awareness/endpoint.html

[13]Wikipedia contributors. (2022a, January 20). Application security. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Application_security&oldid=1066835998

[14]What is network Security? (n.d.). Check Point Software. Retrieved February 22, 2022, from https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

[15]Uctu, G., Alkan, M., Dogru, I. A., & Dorterler, M. (2019). Perimeter network security solutions: A survey. 2019 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT).

[16]Miller, L. (n.d.). Human Layer Security. Egress.Com. Retrieved February 22, 2022, from https://www.egress.com/media/qqznmb5p/egress-human-layer-security-for-dummies.pdf

[17](Canadian Centre for Cyber Security, 2018)

Canadian Centre for Cyber Security. (2018, August 15). Cyber threat and cyber threat actors. Canadian Centre for Cyber Security. https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors

[18]S. Bhunia, M. S. Hsiao, M. Banga and S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1229-1247, Aug. 2014, doi: 10.1109/JPROC.2014.2334493.

[19]Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

[20]VirusTotal. (n.d.). Virustotal.Com. Retrieved February 22, 2022, from https://www.virustotal.com/gui/file/

[21]ENISA surveys evolving threat landscape. (2013). Computer Fraud & Security, 2013(1), 1–3. https://doi.org/10.1016/s1361-3723(13)70001-0

[22]EMOTET malware resurges with new detections. (n.d.). Trendmicro.Com. Retrieved February 23, 2022, from https://success.trendmicro.com/solution/1118391-malware-awareness-emotet-resurgence

[23]K. P. Grammatikakis, I. Koufos, N. Kolokotronis, C. Vassilakis and S. Shiaeles, "Understanding and Mitigating Banking Trojans: From Zeus to Emotet," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 121-128, doi: 10.1109/CSR51186.2021.9527960.

[24]Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys, 39(1), 3. https://doi.org/10.1145/1216370.1216373

[25]R. K. C. Chang, "Defending against flooding-based distributed denial-of-service attacks: a tutorial," in IEEE Communications Magazine, vol. 40, no. 10, pp. 42-51, Oct. 2002, doi: 10.1109/MCOM.2002.1039856.

[26]TCP SYN flood. (n.d.). Learning Center. Retrieved February 23, 2022, from https://www.imperva.com/learn/ddos/syn-flood/

[27](A Survey of Man In The Middle Attacks Mauro Conti, Senior Member, n.d.)

A Survey of Man In The Middle Attacks Mauro Conti, Senior Member. (n.d.). IEEE.

[28]Y. Zhao, R. Guo and P. Lv, "ARP Spoofing Analysis and Prevention," 2020 5th International Conference on Smart Grid and Electrical Automation (ICSGEA), 2020, pp. 572-575, doi: 10.1109/ICSGEA51094.2020.00130.

[29](Chen et al., 2010)

Chen, T.-C., Dick, S., & Miller, J. (2010). Detecting visually similar Web pages: Application to phishing detection. ACM Transactions on Internet Technology, 10(2), 1–38. https://doi.org/10.1145/1754393.1754394

[30]M. Khonji, Y. Iraqi and A. Jones, "Phishing Detection: A Literature Survey," in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013, doi: 10.1109/SURV.2013.032213.00009.

[31]L. K. Shar and H. B. K. Tan, "Defeating SQL Injection," in Computer, vol. 46, no. 3, pp. 69-77, March 2013, doi: 10.1109/MC.2012.283.

[32]A. Tajpour and M. J. z. Shooshtari, "Evaluation of SQL Injection Detection and Prevention Techniques," 2010 2nd International Conference on Computational Intelligence, Communication Systems and Networks, 2010, pp. 216-221, doi: 10.1109/CICSyN.2010.55.

[33]D. A. Kindy and A. K. Pathan, "A survey on SQL injection: Vulnerabilities, attacks, and prevention techniques," 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), 2011, pp. 468-471, doi: 10.1109/ISCE.2011.5973873.

[34]A. Sadeghian, M. Zamani and A. A. Manaf, "A Taxonomy of SQL Injection Detection and Prevention Techniques," 2013 International Conference on Informatics and Creative Multimedia, 2013, pp. 53-56, doi: 10.1109/ICICM.2013.18.

[35]Sruthi Bandhakavi, Prithvi Bisht and P. Madhusudan, CANDID: Preventing SQL Injection Attacks using Dynamic Candidate Evaluations, Alexandria, Virginia, USA:ACM, 2007.

[36]Prithvi Bisht and P. Madhusudan, "CANDID: Dynamic Candidate Evaluations for Automatic Prevention of SQL Injection Attacks", Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 1-38, 2007

[37](Bisht et al., 2010)

Bisht, P., Madhusudan, P., & Venkatakrishnan, V. N. (2010). CANDID: Dynamic candidate evaluations for automatic prevention of SQL injection attacks. ACM Transactions on Information and System Security, 13(2), 1–39. https://doi.org/10.1145/1698750.1698754

[38]R. A. McClure and I. H. Kruger, "SQL DOM: compile time checking of dynamic SQL statements," Proceedings. 27th International Conference on Software Engineering, 2005. ICSE 2005., 2005, pp. 88-96, doi: 10.1109/ICSE.2005.1553551.

[39]R.A. McClure and I.H. Kruger, "SQL DOM: compile time checking of dynamic SQL statements", Software Engineering 2005. ICSE 2005. Proceedings. 27th International Conference on, pp. 88-96, 15–21 May 2005.

[40](Kemalis & Tzouramanis, 2008)

Kemalis, K., & Tzouramanis, T. (2008). SQL-IDS: A specification-based approach for SQL-injection detection. Proceedings of the 2008 ACM Symposium on Applied Computing - SAC '08.

[41]J. Vukalović and D. Delija, "Advanced Persistent Threats - detection and defense," 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015, pp. 1324-1330, doi: 10.1109/MIPRO.2015.7160480.

[42](National Institute of Standards and Technology, 2018)

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. National Institute of Standards and Technology.

[43](CIS critical security Controls, n.d.)

CIS critical security Controls. (n.d.). CIS. Retrieved February 23, 2022, from https://www.cisecurity.org/controls

[44](Higher education community vendor assessment toolkit, n.d.)

Higher education community vendor assessment toolkit. (n.d.). Educause.Edu. Retrieved February 23, 2022, from https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit

[45](Lynch et al., n.d.)

Lynch, B., Zongker, J., Hewitt, N., Manor, M., & Pappalexis, J. (n.d.). Iso/iec 27001. Learning Center. Retrieved February 23, 2022, from https://www.imperva.com/learn/data-security/iso-27001/

[46](ISO 27001, the information security standard made easy, n.d.)

ISO 27001, the information security standard made easy. (n.d.). Retrieved February 23, 2022, from https://www.isms.online/iso-27001/

[47](Wikipedia contributors, 2021a)

Wikipedia contributors. (2021a, December 17). ISO/IEC 27001. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=ISO/IEC_27001&oldid=1060727632

[48](Singare & Tembhurkar, n.d.)

Singare, Y., & Tembhurkar, M. (n.d.). Sciences s s s and Engineering and Engineering and Engineering and Engineering Open Access. Ijcseonline.Org. Retrieved February 23, 2022, from https://www.ijcseonline.org/pub_paper/9-IJCSE-00702.pdf

[49]Ometov, Aleksandr & Bezzateev, Sergey & Mäkitalo, Niko & Andreev, Sergey & Mikkonen, Tommi & Koucheryavy, Yevgeni. (2018). Multi-Factor Authentication: A Survey. Cryptography. 2. 10.3390/cryptography2010001.

[50](BarbaraSelden, n.d.)

BarbaraSelden. (n.d.). NIST authentication basics. Microsoft.Com. Retrieved February 23, 2022, from https://docs.microsoft.com/en-us/azure/active-directory/standards/nist-authentication-basics

[51](Huseynov & Seigneur, 2015)

Huseynov, E., & Seigneur, J.-M. (2015). WiFiOTP: Pervasive two-factor authentication using Wi-Fi SSID broadcasts. 2015 ITU Kaleidoscope: Trust in the Information Society (K-2015).

[52]J. Bonneau, "The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords", 2012 IEEE Symposium on Security and Privacy, pp. 538-552, 2012.

[53]J. Bonneau and S. Preibusch, "The password thicket: technical and market failures in human authentication on the web", WEIS '10: Proceedings of the 9 Workshop on the Economics of Information Security, 2010.

Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication? | IEEE Conference Publication | IEEE Xplore (ualberta.ca)

[54](Messente Communications Ltd, n.d.)

Messente Communications Ltd. (n.d.). What are the benefits of two-factor authentication? Messente.Com. Retrieved February 23, 2022, from https://messente.com/blog/most-recent/benefits-of-two-factor-authentication

[55](McKeever et al., n.d.)

McKeever, G., Lynch, B., Hewitt, N., Vitaly, Daniel, Nathan, & Rossi, E. (n.d.). What is Two Factor Authentication. Learning Center. Retrieved February 23, 2022, from https://www.imperva.com/learn/application-security/2fa-two-factor-authentication/

[56](Hammood et al., 2020)

Hammood, W. A., Abdullah, R., Hammood, O. A., Mohamad Asmara, S., Al-Sharafi, M. A., & Muttaleb Hasan, A. (2020). A review of user authentication model for online banking system based on mobile IMEI number. IOP Conference Series. Materials Science and Engineering, 769(1), 012061. https://doi.org/10.1088/1757-899x/769/1/012061

[57]Introduction to certificate-based authentication (sun directory server enterprise edition 7.0 reference). (n.d.). Oracle.Com. Retrieved February 22, 2022, from https://docs.oracle.com/cd/E19424-01/820-4811/gdzdg/index.html

[58]Wikipedia contributors. (2022b, February 18). Public key certificate. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Public_key_certificate&oldid=1072483251

[59]Albarqi, A., Alzaid, E., Ghamdi, F. A., Asiri, S., & Kar, J. (2015). Public Key Infrastructure: A Survey. Journal of Information Security, 06(01), 31–37. https://doi.org/10.4236/jis.2015.61004

[60]Harris, J. (n.d.). Using Certificate-based Authentication for Access Control. Globalsign.Com. Retrieved February 22, 2022, from https://www.globalsign.com/en/resources/white-paper-certificate-based-authentication-for-access-control.pdf

[61]A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.

[62]Choudhury, B., Then, P., Issac, B., Raman, V., & Haldar, M. K. (2018). A survey on biometrics and cancelable biometrics systems. International Journal of Image and Graphics, 18(01), 1850006. https://doi.org/10.1142/s0219467818500067

[63]Harakannanavar, S. S., Renukamurthy, P. C., & Raja, K. B. (2019). Comprehensive study of biometric authentication systems, challenges and future trends. International Journal of Advanced Networking and Applications, 10(4), 3958–3968. https://doi.org/10.35444/ijana.2019.10048

[64]Magrath, M. (n.d.). Biometric facial recognition software: Massive gains in accuracy, but challenges remain. OneSpan. Retrieved February 22, 2022, from

https://www.onespan.com/blog/biometric-facial-recognition-software-massive-gains-accuracy-challenges-remain

[65]Wikipedia contributors. (2021, December 18). Eigenface. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Eigenface&oldid=1060853235

[66]Thakkar, D. (2016, October 21). Minutiae based extraction in fingerprint recognition. Bayometric. https://www.bayometric.com/minutiae-based-extraction-fingerprint-recognition/

[67]Faundez-Zanuy, M., & Mérida, G. M. N. (2005). Biometric identification by means of hand geometry and a neural net classifier. In Computational Intelligence and Bioinspired Systems (pp. 1172–1179). Springer Berlin Heidelberg.

[68]Wikipedia contributors. (2022, January 30). Biometrics. Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Biometrics&oldid=1068841762

[69]Haskett, M. (2017, June 22). Biometrics 101: Iris recognition vs. Retina scanning. Medium. https://mary-haskett.medium.com/biometrics-101-iris-recognition-vs-retina-scanning-3469349b0eb3

[70]Wilson, Y., & Hingnikar, A. (2019). Solving identity management in modern applications: Demystifying OAuth 2.0, OpenID connect, and SAML 2.0 (1st ed.). APress.

[71]C. DeCusatis, P. Liengtiraphan, A. Sager and M. Pinelli, "Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication," 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp. 5-10, doi: 10.1109/SmartCloud.2016.22.

[72]M. Shore, S. Zeadally and A. Keshariya, "Zero Trust: The What, How, Why, and When," in Computer, vol. 54, no. 11, pp. 26-35, Nov. 2021, doi: 10.1109/MC.2021.3090018.

[73]Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standards and Technology.

[74]S. Mehraj and M. T. Banday, "Establishing a Zero Trust Strategy in Cloud Computing Environment," 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104214.

Single Sign On

[75] Okereafor, K., 2021. Cybersecurity in the COVID-19 Pandemic. Milton: Taylor & Francis Group.

[76] Z. Ahmed and S. C. Francis, "Integrating Security with DevSecOps: Techniques and Challenges," 2019 International Conference on Digitization (ICD), 2019, pp. 178-182, doi: 10.1109/ICD47981.2019.9105789.

[77] E. C. Burkard, "Usability Testing within a Devsecops Environment," 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), 2020, pp. 1C1-1-1C1-7, doi: 10.1109/ICNS50378.2020.9222919.

[78] Abrahamsson, P., Botterweck, G., Ghanbari, H., Jaatun, M., Kettunen, P., Mikkonen, T., Mjeda, A., Münch, J., Duc, A., Russo, B. and Wang, X., 2020. Towards a Secure DevOps Approach for Cyber-Physical Systems. International Journal of Systems and Software Security and Protection, 11(2), pp.38-57.

[79]RIBEIRO, M., 2022. LEARNING DEVSECOPS. [S.l.]: O'REILLY MEDIA.

[80]Docs.broadcom.com. 2022. [online] Available at: https://docs.broadcom.com/doc/managed-security-services-en.

[81]Docs.broadcom.com. 2022. [online] Available at: https://docs.broadcom.com/doc/integrated-cyber-defense-solution-brief.

[82]2022. [online] Available at: https://www.akamai.com/resources/product-brief/managed-security-service-product-brief

[83]Gibson, D., 2014. Managing Risk in Information Systems, 2nd Edition. 2nd ed. Jones & Bartlett Learning.

[84]Sutton, D., 2017. Cyber Security. BCS Learning & Development Limited.

[85] D. Kasap and M. Kaymak, "Risk Identification Step of the Project Risk Management," PICMET '07 - 2007 Portland International Conference on Management of Engineering & Technology, 2007, pp. 2116-2120, doi: 10.1109/PICMET.2007.4349543.

[86]2011. Managing information security risk. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.

[87] L. Wilbanks, "Whats Your IT Risk Approach?," in IT Professional, vol. 20, no. 4, pp. 13-17, Jul./Aug. 2018, doi: 10.1109/MITP.2018.043141663.

[88]Z. A. Collier, D. DiMase, S. Walters, M. M. Tehranipoor, J. H. Lambert and I. Linkov, "Cybersecurity Standards: Managing Risk and Creating Resilience," in Computer, vol. 47, no. 9, pp. 70-76, Sept. 2014, doi: 10.1109/MC.2013.448.

[89]J. R. C. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems," in IT Professional, vol. 19, no. 5, pp. 20-26, 2017, doi: 10.1109/MITP.2017.3680959.

[90]P. H. Meland, I. A. Tondel and B. Solhaug, "Mitigating Risk with Cyberinsurance," in IEEE Security & Privacy, vol. 13, no. 6, pp. 38-43, Nov.-Dec. 2015, doi: 10.1109/MSP.2015.137.

[91]L. Xiaosong, L. Shushi, C. Wenjun and F. Songjiang, "The Application of Risk Matrix to Software Project Risk Management," 2009 International Forum on Information Technology and Applications, 2009, pp. 480-483, doi: 10.1109/IFITA.2009.542.