Tracing The Timeline of Network Security From the 1950s To the Present (2023)

Deepanshu Jain & Ankur Sheth
3rd Year Computer Science and Engineering Undergraduates
Manipal University Jaipur, Rajasthan, India

***Abstract* — The field of network security has evolved significantly over the years, with new threats emerging and security measures adapting in response. Network security problems exist through all the layers of the computer network, and the network security objective is to maintain the confidentiality, authenticity, integrity, dependability, availability, and suitability of the network. The rapid development of computer network systems brings both great convenience and new security threats for users. Network security problems generally include network system security and data security. Specifically, it refers to the reliability of the network system, confidentiality, integrity, and availability of data information in the system. This paper aims to trace the timeline of network security in chronological order, starting from the early days of computing to the present day. The paper will explore the major milestones in the development of network security, including the emergence of viruses, the introduction of firewalls, and the rise of cybercrime. By examining the historical context of these developments, this paper will provide a deeper understanding of the evolution of network security and the challenges that continue to shape the field today. Ultimately, this paper will demonstrate how network security has become an essential component of modern computing, and how its evolution has helped shape the digital world we live in today.**

***Index Terms* — Access Control, Anti-Virus, Asymmetric Key, Authentication, Availability, Cipher, Clearance levels, Confidentiality, Data encryption, DevSecOps, Firewalls, Firmware, Hash Function, IDS, Integrity, Intrusion, NAT, Security, Security Audits, SOAR, Symmetric Key, VPN, XDR**

1. An Introduction to Security

1a. What is Security in literature terms?

Security is protection from, or resilience against, potential harm (or other unwanted coercive) caused by others, by restraining the freedom of others to act. Beneficiaries (technically referents) of security may be persons and social groups, objects, institutions, ecosystems, or any other entity or phenomenon vulnerable to unwanted change. Security mostly refers to protection from hostile forces, but it has a wide range of other senses: for example, the absence of harm (e.g. freedom from want); the presence of an essential good (e.g. food security); as resilience against potential damage or harm (e.g. secure foundations); as secrecy (e.g. a secure telephone line); as containment (e.g. a secure room or cell); and as a state of mind (e.g. emotional security). The term is also used to refer to acts and systems whose purpose may be to provide security (security company, security forces, security guard, cyber security systems, security cameras, remote guarding). Security can be physical or virtual. On a governance level, security is a defining characteristic of a society as a fundamental function of the state and a necessary condition to allow the enjoyment and exercise of rights and freedoms pursued by the rule of law.

1b. What is Security in terms of Computer Science?

Computer security or **Cybersecurity** refers to protecting and securing computers and their related data, networks, software, and hardware from unauthorized access, misuse, theft, information loss, and other security issues. The Internet has made our lives easier and has provided us with lots of advantages, but it has also put our system's security at risk of being infected by a virus, being hacked, information theft, damage to the system, and much more. Technology is growing day by day and the entire world is in its grasp. We cannot imagine even a day without electronic devices around us. With the use of this growing technology, invaders, hackers, and thieves are trying to harm our computer's security for monetary gains, recognition purposes, ransom demands, bullying others, invading other businesses, organizations, etc. To protect our system from all these risks, computer security is important.

There are several types of computer security which is widely used to protect the valuable information of an organization. One way to ascertain the similarities and differences in Computer Security is by asking what is being secured. For example,

- *Information Security* is securing information from unauthorized access, modification & deletion.
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches, etc.
- *Internet Security* establishes rules and measures to use against attacks over the Internet.
- *Network Security* is by securing both the software and hardware technologies.
- *Endpoint Security* is an approach to the protection of

computer networks that are remotely bridged to client devices.

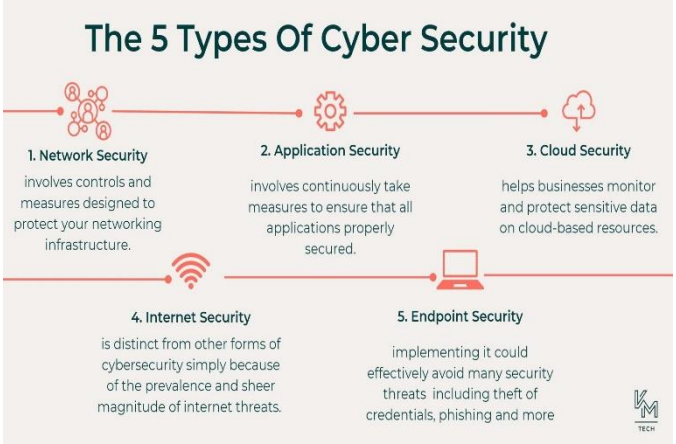


Fig. 1 The 5 Types of Cyber Security
Link Ref- https://kmtech.com.au/wp-content/uploads/2022/04/The-5-Types-Of-Cyber-Security-2048x1024.jpg

It is important to understand the distinction between these words, though there is not necessarily a clear consensus on the meanings and the degree to which they overlap or are interchangeable.

So, **Computer security** or **Cybersecurity** can be defined as controls that are put in place to provide *confidentiality*, *integrity*, and *availability* for all components of computer systems. Let us elaborate on the definition.

Components of computer system

The components of a computer system that needs to be protected are:

- *Hardware*, the physical part of the computer, like the system memory and disk drive
- *Firmware*, permanent software that is etched into a hardware device's non-volatile memory and is mostly invisible to the user.
- *Software*, the programming that offers services, like operating systems, word processors, and internet browsers to the user.

The CIA Triad

Computer security is concerned with three principal areas:

- *Confidentiality is* ensuring that information is available only to the intended audience.
- *Integrity is* protecting information from being modified by unauthorized parties.
- *Availability is* protecting information from being modified by unauthorized parties.

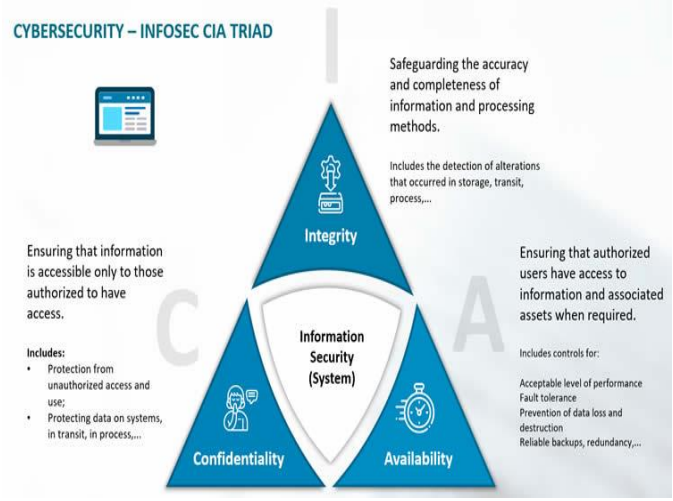


Fig. 2 The CIA Triad
Link Ref - https://www.i-scoop.eu/wp-content/uploads/2022/04/Cybersecurity-the-infosec-CIA-Triad.jpg

In simple language, computer security is making sure information and computer components are usable but still protected from people or software that should not access or modify them.

2. TYPES OF SECURITY

2a. Information Security

Information security is a type of cyber security that specially focuses on the methodology and techniques that are built for ensuring computer security. Information security, as a Process was developed to protect the availability, integrity, and confidentiality of computer systems from Data thefts, unauthorized access, harm, and destruction. Information security is commonly known as the CIA triad and this model is used for protecting the integrity, availability, and confidentiality of organizational data so that productivity is maintained.

2b. Application Security

When security features are introduced in the primary stage of the development process, that is one it is known as application security. It is very well capable of protecting your computer system from cyber security threats such as unauthorized access and data breaches. Furthermore, it can also help your computer system to fight against SQL breaches and denial of service

attacks. Some of the major application tools techniques are used for installing the application security feature, such as software encryption, antivirus, firewall, etc. and these help your system to build a wall against cyber-attacks.

2c. Internet Security

Internet security is the most recent type of computer security that has reached a boom period in recent times. It is a method for creating a perfect set of rules and actions to prevent any unauthorized use or harm to computer systems that are directly connected to the internet. Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the Internet. These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers. Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.

2d. Network Security

Network security as the name suggests is another type of computer security that protects your computer system from authorized intrusions and access to your computer networks. It is like information security in way that it also protects the integrity, availability, and confidentiality of your computer networks. Network security is designed in a way with a lot of configurations that it performs to its best abilities. it includes the safety of both Software and hardware.

2e. Endpoint security

Endpoint security is the practice of securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats. Endpoint security has evolved from traditional antivirus software to providing comprehensive protection from sophisticated malware and evolving zero-day threats. Organizations of all sizes are at risk from nation-states, hacktivists, organized crime, and malicious and accidental insider threats. Endpoint security is often seen as cybersecurity's frontline and represents one of the first places organizations look to secure their enterprise networks.

3. History and Development of Network Security

3a. From 1950 to 1970

In the 1950s, network security was a new concept, and computer networks were limited to a small number of specialized systems used by government and academic institutions. At the time, security was primarily focused on physical security, such as protecting the computer equipment itself and the data stored on it.

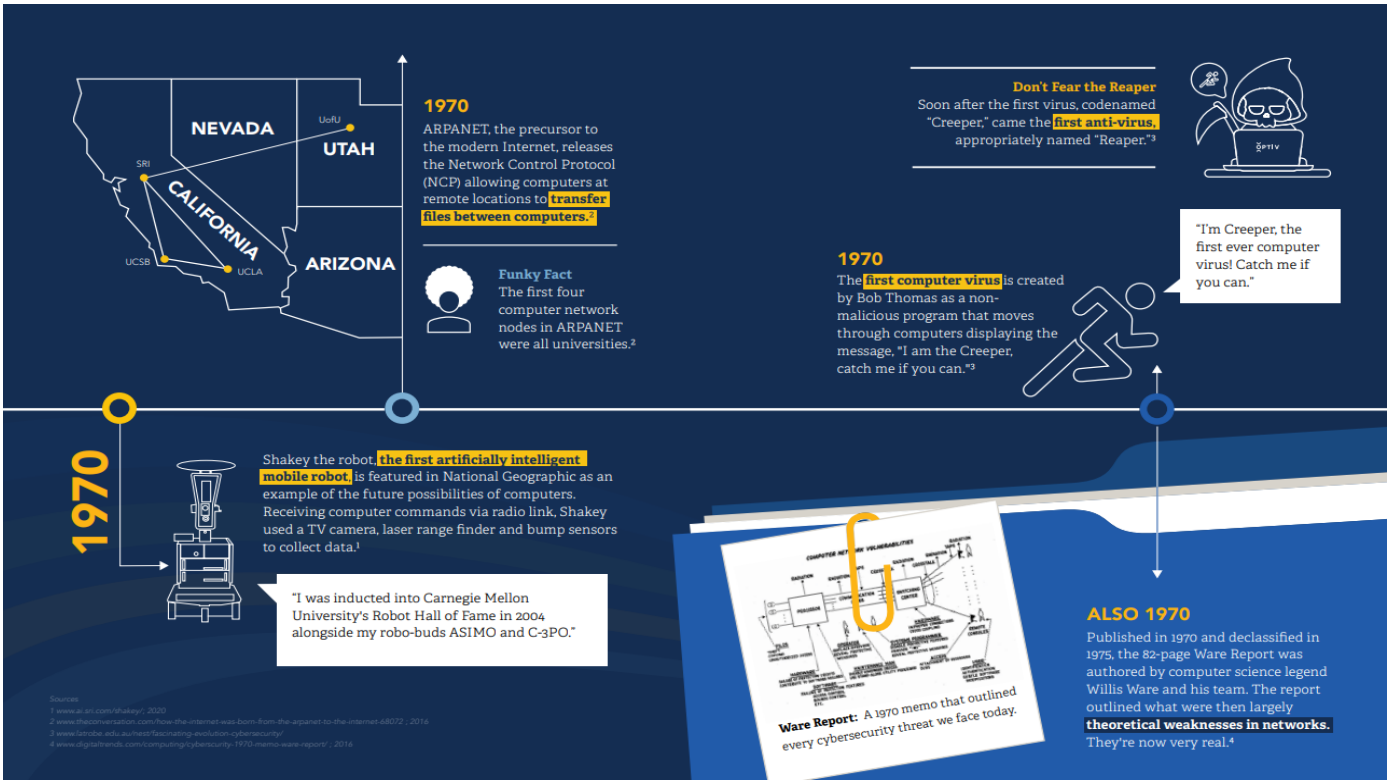
There were no standardized methods or technologies for protecting computer networks, so each organization would develop its security measures, such as:

1. *Access Control:* Access to computer systems was limited to a small number of authorized users, who were typically required to have an elevated level of clearance. Passwords were used to authenticate users and limit access to sensitive data.
2. *Data Encryption:* Data transmitted over networks was often encrypted to protect it from being intercepted and read by unauthorized users.
3. *Firewalls:* Some organizations used firewalls to protect their networks from external threats by limiting incoming and outgoing network traffic based on predefined rules.

Access Control:

Despite these measures, computer security was still in its infancy in the 1950s, and many networks were vulnerable to attacks from both internal and external sources. As a result, security was often seen as an afterthought, rather than a priority, in the early days of computing. In the 1950s, access control to computer to prevent unauthorized access to computer equipment, while procedural measures including the use of passwords and clearance levels to regulate access to sensitive data.

1. *Passwords:* Passwords were used to authenticate users and grant them access to the computer system. Passwords were typically assigned by the system administrator and were kept confidential.
2. *Clearance Levels:* Access to sensitive data was typically restricted based on a user's clearance level, which was determined by their position and responsibilities within the organization. Users with higher clearance levels would have access to more sensitive data than those with lower clearance levels.
3. *Limited Access:* Access to computer systems was limited to a small number of authorized users, and each user was typically assigned specific permissions and responsibilities. This helped to prevent unauthorized access to sensitive data and reduce the risk of security breaches.



Data Encryption:

In the 1960s, computer systems were often large, centralized mainframes that were shared by multiple users, so it was important to have strict controls in place to prevent unauthorized access and protect sensitive data. However, these controls were not foolproof and could be bypassed by determined attackers, so organizations still needed to be vigilant and take other security measures, such as data encryption, to protect their systems and data.

In the 1960s, data encryption was a new concept, and the methods used to encrypt data were not as advanced as they are today. At the time, encryption was primarily used to protect sensitive information transmitted over communication networks, such as teletypes and leased lines.

1. *Symmetric Key Encryption:* Symmetric key encryption was the most common method used for data encryption in the 1960s. In this method, the same key was used for both encryption and decryption, and both the sender and receiver of the data needed to have access to the key.
2. *Cryptographic Algorithms:* A few basic cryptographic algorithms, such as the Caesar Cipher and the Vigenère Cipher, were used to encrypt data. These algorithms were simple and easy to use, but they were also relatively easy to crack and not considered secure by modern standards.
3. *Key Exchange:* Key exchange was a major challenge in the 1960s, as there was no secure way to exchange keys between the sender and receiver of encrypted data. This made it difficult to ensure that the intended recipient could only read encrypted data.

Overall, data encryption in the 1960s was in its initial stages and not as robust as it is today. Despite these limitations, encryption was still considered a valuable tool for protecting sensitive information transmitted over networks, and it was a crucial step toward the development of more secure encryption methods in the future.

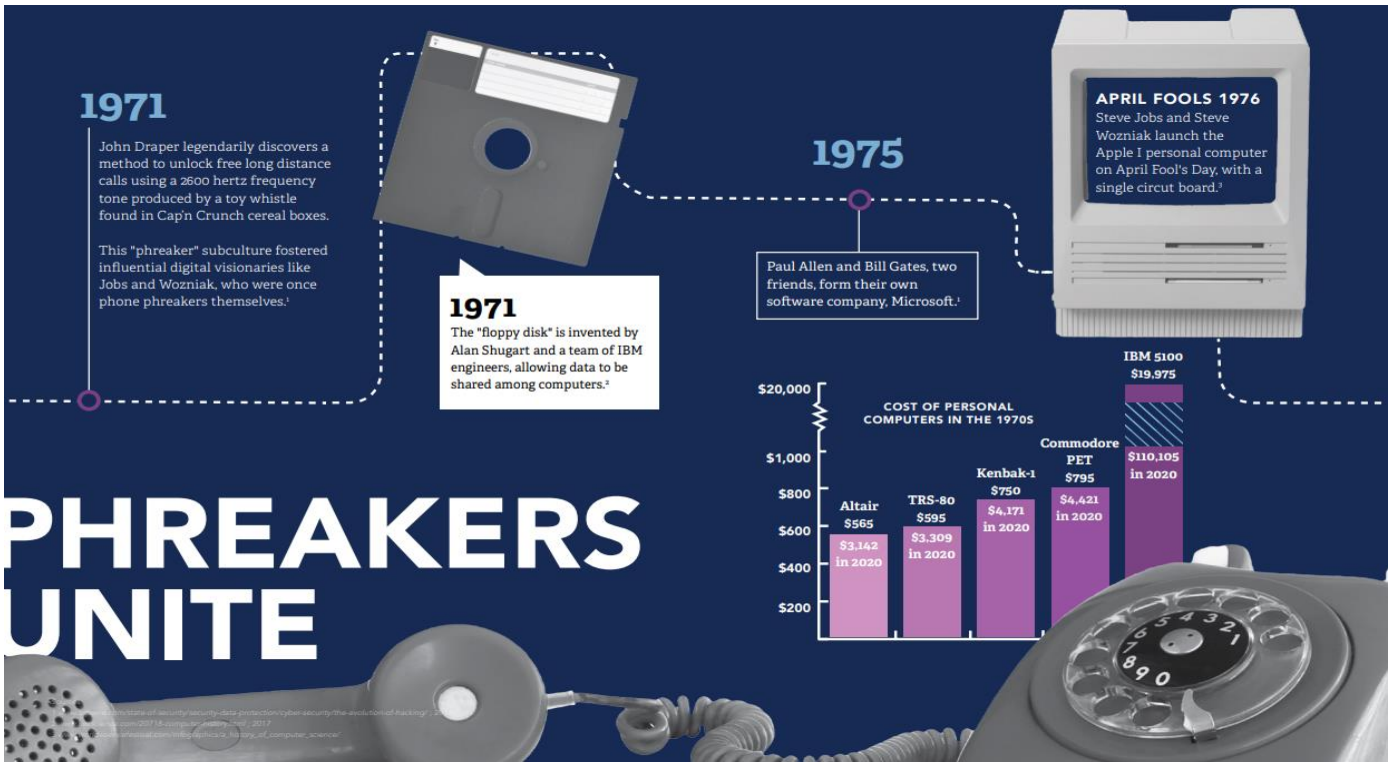
3b. In the 1970s

Fig. 3 Some important milestones and events in the 1970s Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 5

In the 1970s, network security became increasingly important as computer networks grew and complexity and began to be used for a wider range of applications, including financial transactions and military communications. Some of the security measures used in the 1970s included:

1. *Access Control:* Access control to computer systems became more sophisticated, with the introduction of role-based access control and the use of multi-factor authentication, such as passwords and smart cards.
2. *Data Encryption:* The use of data encryption continued to be an important aspect of network security in the 1970s, with the development of more advanced encryption algorithms, such as the Data Encryption Standard (DES).

Firewalls: The concept of firewalls as network **Fig. 4** Some



important milestones and events in the 1970s

Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 6

3. security tools became more widely adopted, with the introduction of the first commercial firewalls, such as the TIS firewall. Firewalls were used to limit incoming and outgoing network traffic and prevent unauthorized access to internal networks.
4. *Security Audits:* Security audits became more systematic and comprehensive, with the development of security frameworks and methodologies for conducting security assessments.

Despite these advances, network security was still a challenge in the 1970s, and many networks were vulnerable to attacks from both internal and external sources. As a result, security continued to be seen as an afterthought in many organizations, rather than a priority. Nevertheless, the 1970s were an important decade for the development of network security, as the foundation for many of the security measures and technologies used today was established during this time.

Access Control:

In the 1970s, access control to computer systems became more sophisticated and was an important aspect of network security. Some of the methods used to achieve access control in the 1970s included:

1. *Role-based access control:* This approach to access control assigned various levels of access to different users based on their roles within the organization. For example, a system administrator might have more privileges than a regular user.
2. *Multi-factor authentication:* In addition to passwords, other forms of authentication, such as smart cards, were used to provide an extra level of security and make it more difficult for unauthorized users to access computer systems.
3. *Access logs:* Access logs were used to keep track of who had accessed the system and what they had done, providing an audit trail that could be used to detect and respond to security breaches.
4. *Physical security:* Physical security measures, such as locked computer rooms and secure storage for backup media, were used to protect computer systems and data from theft and unauthorized access.

These measures helped to improve access control to computer systems in the 1970s, but security was still a challenge, and many networks were vulnerable to attacks from both internal and external sources. As a result, access control was often seen to limit damage in the event of a security breach, rather than as an initiative-taking measure to prevent security breaches from happening in the first place. Nevertheless, the 1970s were an important decade for the development of access control, as the foundation for many of the access control methods and technologies used today was established during this time.

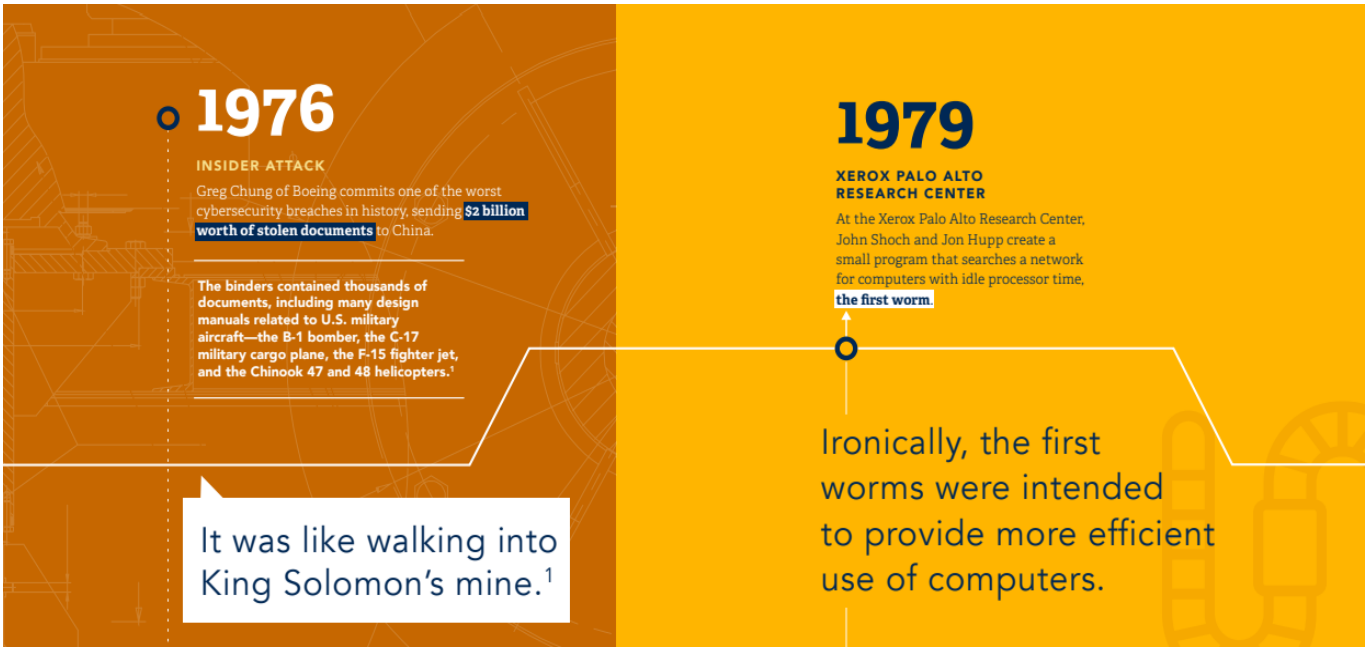


Fig. 5 Some important milestones and events in the 1970s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 7

Data Encryption:

In the 1970s, data encryption was an important aspect of network security, as computer networks became larger and more complex, and sensitive information needed to be transmitted over these networks. Some of the methods used for data encryption in the 1970s included:

1. *Symmetric-key encryption:* Symmetric-key encryption algorithms, such as the Data Encryption Standard (DES), were widely used for data encryption in the 1970s. In symmetric-key encryption, the same key is used to encrypt and decrypt the data, making it fast and efficient but also vulnerable to key compromise.
2. *Key exchange:* Key exchange methods were used to securely exchange encryption keys between parties over an insecure communication channel. Key exchange methods, such as Diffie-Hellman, provided a secure way to exchange encryption keys without exposing them to attackers.
3. *Cryptographic protocols:* Cryptographic protocols, such as the Secure Sockets Layer (SSL) and Transport Layer Security (TLS), were developed to provide secure communication over networks. These protocols used data encryption and other security measures to protect sensitive information transmitted over the network.

Data encryption in the 1970s helped to protect sensitive information transmitted over computer networks and prevented unauthorized access to that information. However, security was still a challenge, and many networks were vulnerable to attacks from both internal and external sources. As a result, data encryption was often seen to limit damage in the event of a security breach, rather than as an initiative-taking measure to prevent security breaches from happening in the first place. Nevertheless, the 1970s were an important decade for the development of data encryption, as the foundation for many of the encryption algorithms and technologies used today was established during this time.

Firewalls:

In the 1970s, firewalls became an increasingly important aspect of network security, as computer networks grew and complexity and began to be used for a wider range of applications, including financial transactions and military communications.

1. *First commercial firewalls:* The first commercial firewalls, such as the TIS security system, were introduced in the 1970s. These firewalls were used to limit incoming and outgoing network traffic and prevent unauthorized access to internal networks.
2. *Packet filtering:* Packet filtering was a commonly used method for firewalls in the 1970s. This involved examining the header of each network packet and allowing or blocking it based on a set of rules, such as the source and destination IP addresses and ports.
3. *Network Address Translation (NAT):* NAT was developed to share a single public IP address among multiple internal systems. NAT allowed firewalls to hide the internal network and prevent unauthorized access from the Internet.

Despite the use of firewalls, security was still a challenge in

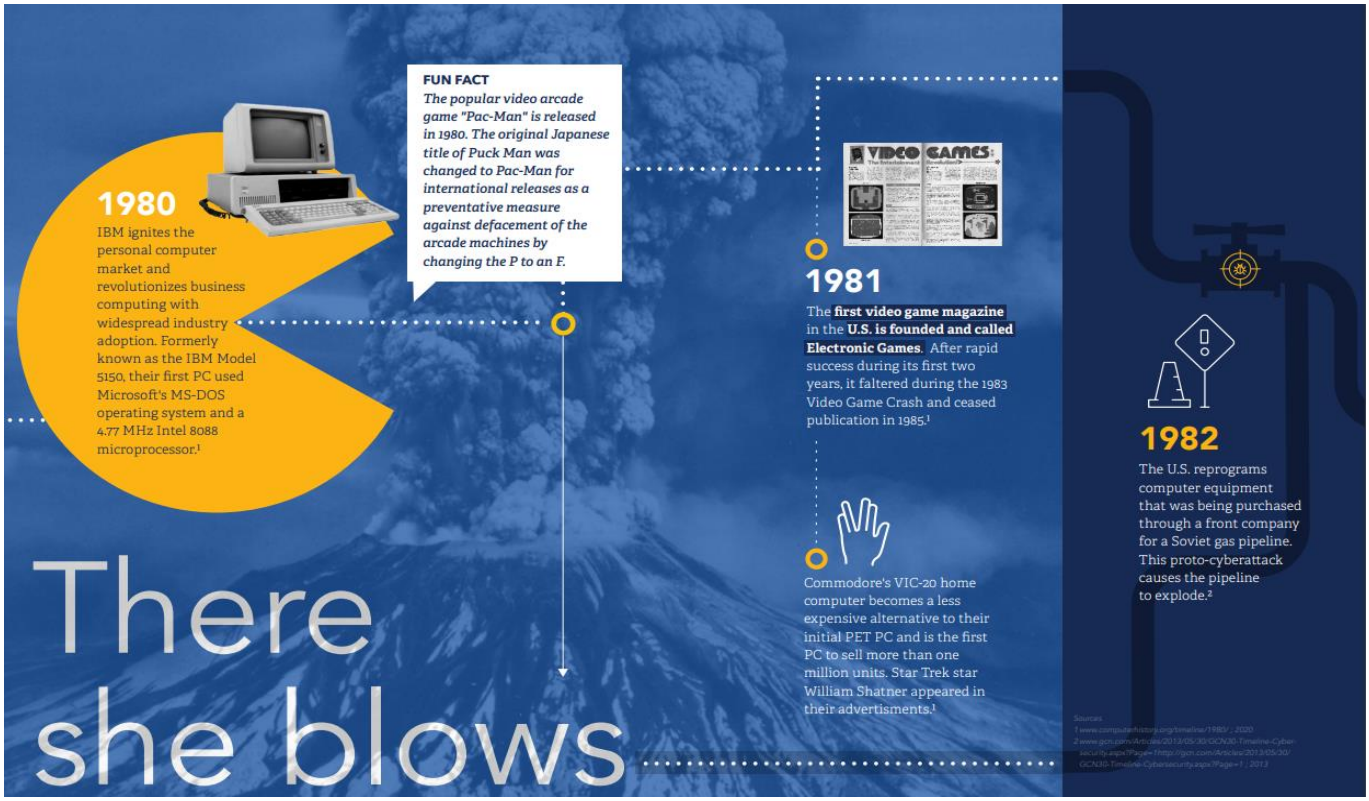


Fig. 6 Some important milestones and events in the 1980s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 9

the 1970s, and many networks were vulnerable to attacks from both internal and external sources. As a result, firewalls were often seen to limit damage in the event of a security breach, rather than as an initiative-taking measure to prevent security breaches from happening in the first place. Nevertheless, the 1970s were.

an important decade for the development of firewalls, as the foundation for many of the security system technologies and methods used today was established during this time.

3c. In 1980s

In the 1980s, network security became an increasingly critical issue, as computer networks became more widespread and were used for a wider range of applications, including financial transactions and military communications. Some of the new methods besides previously used techniques, used to achieve network security in the 1980s included:

1. *Intrusion detection:* Intrusion detection systems (IDS) was introduced in the 1980s, providing a way to detect and respond to security breaches in real-time.
2. *Network management:* Network management tools were developed to provide a centralized way to manage and monitor computer networks, helping to improve network security and reduce the risk of security breaches.
3. *Security Audits:* Some organizations conducted security audits to identify vulnerabilities in their computer systems and networks, and to implement measures to reduce the risk of security breaches.

The 1980s saw important developments in network security, as methods and technologies were introduced that provided a more comprehensive and sophisticated approach to network security. Despite these advances, security was still a challenge, and many networks were vulnerable to attacks from both internal and external sources. Nevertheless, the 1980s were an important decade for the development of network security, as the foundation for many of the network security methods and technologies used today was established during this time.

Intrusion Detection:

Intrusion detection was first introduced in the 1980s to detect and respond to security breaches in real time. In the early days of intrusion detection, the methods used were basic and typically relied on manual inspection of logs and other system activity data to identify security threats.

1. *Rule-based intrusion detection:* Rule-based intrusion detection systems were the first type of intrusion detection systems (IDS) used in the 1980s. These systems worked by examining incoming network traffic and comparing it to a set of predefined rules to identify malicious activity.

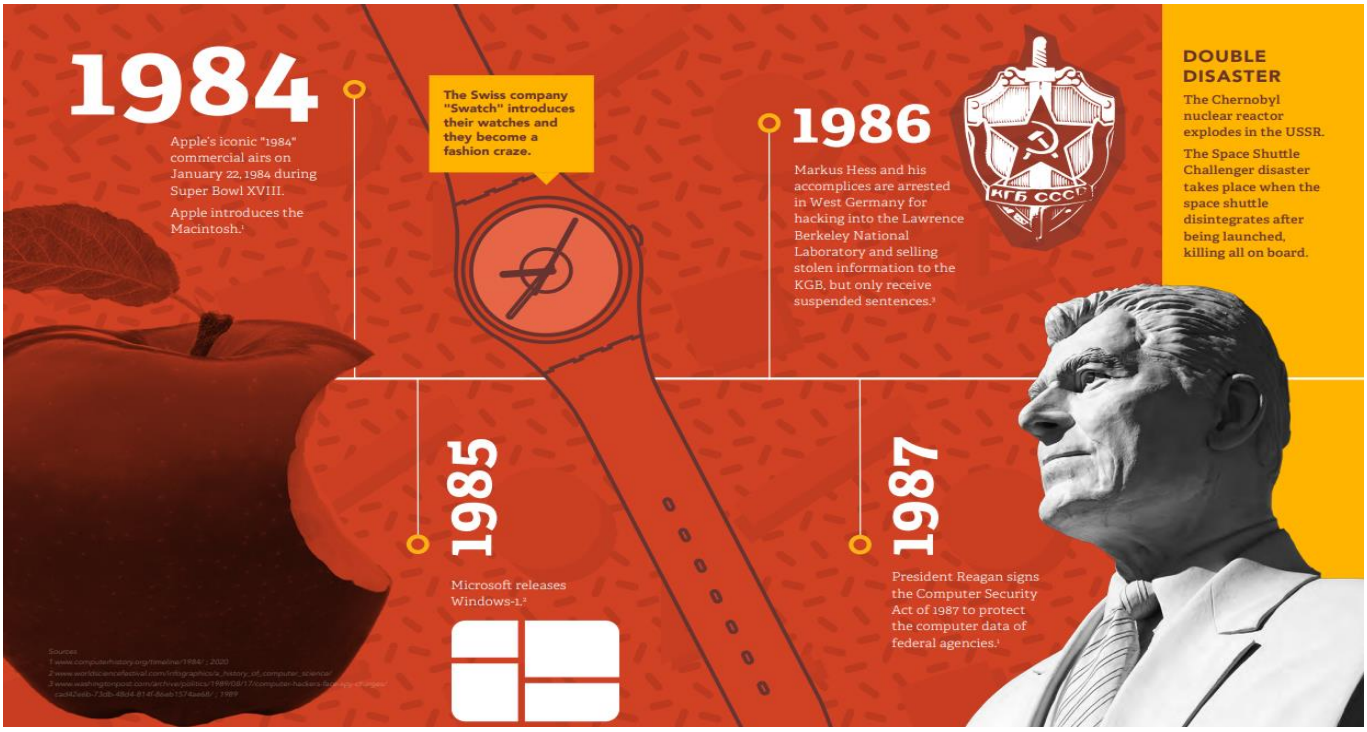


Fig. 7 Some important milestones and events in the 1980s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 10

2. *Signature-based intrusion detection:* Signature-based intrusion detection systems were introduced in the 1980s and became widely used. These systems work by using a database of known attack signatures to identify malicious activity.
3. *Anomaly-based intrusion detection:* Anomaly-based intrusion detection systems were developed in the 1980s to identify new and previously unseen attacks. These systems worked by identifying unusual or unexpected behavior in the network, such as copious amounts of incoming traffic from a single IP address, and raising an alarm in response.

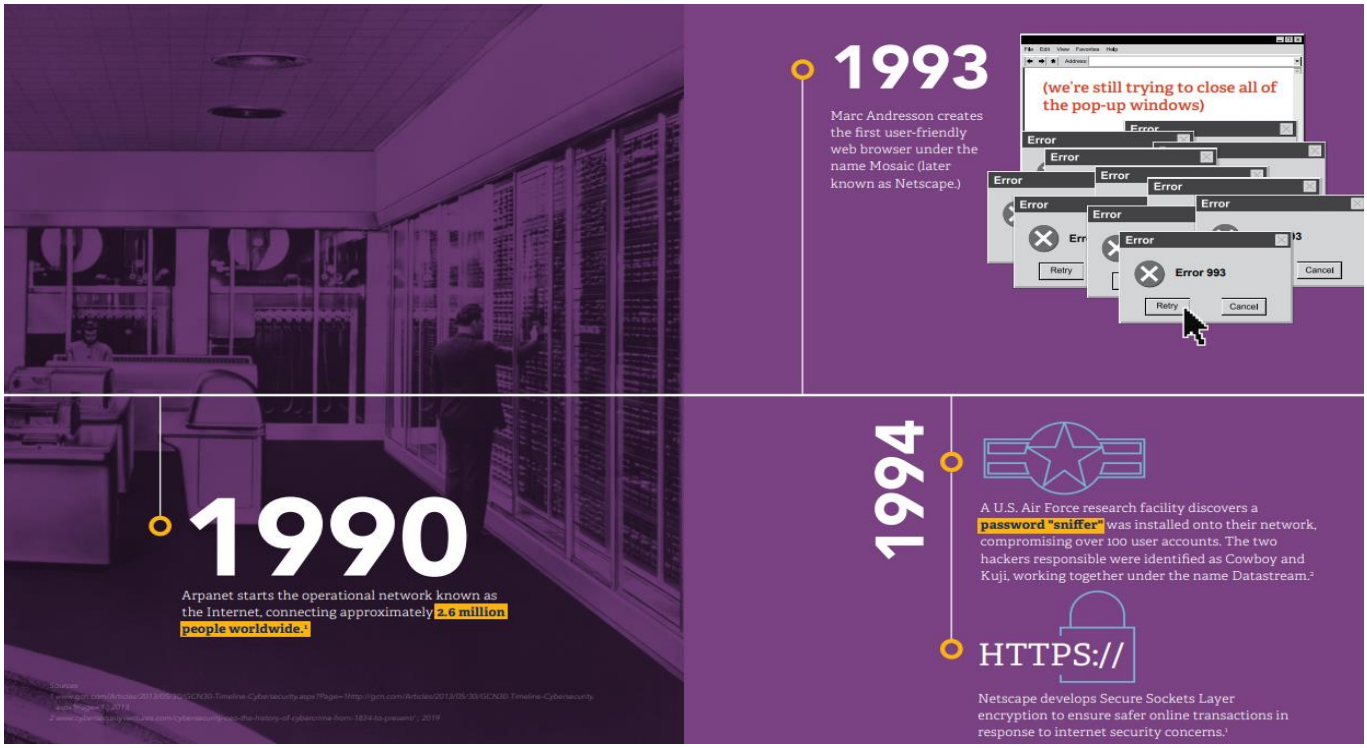
Intrusion detection in the 1980s was still in its infancy, and the methods used were basic compared to those used today. Nevertheless, the development of intrusion detection systems marked a crucial step forward in the evolution of network security, providing a way to detect and respond to security breaches in real-time.

Network Management:

Network management in the 1980s was primitive compared to today's standards, but it was still a crucial aspect of maintaining and securing computer networks. In the 1980s, network management focused on the following areas:

1. *Configuration management:* Configuration management was used to keep track of the configuration of devices on the network and ensure that they were configured correctly.
2. *Performance monitoring:* Performance monitoring was used to monitor the performance of the network and identify bottlenecks or other performance issues that could impact network reliability.
3. *Fault management:* Fault management was used to identify and diagnose faults on the network and resolve them promptly.
4. *Security management:* Security management was used to monitor the network for security breaches and respond to security incidents promptly.
5. *Capacity planning:* Capacity planning was used to ensure that the network could support the growing demand for network resources, such as bandwidth and storage.

In the 1980s, network administrators typically performed network management using a combination of manual processes and simple tools, such as command-line utilities and basic monitoring software. Despite the limitations of the tools and methods available, network management was still an important aspect of maintaining and securing computer networks in the



1980s. The development of network management techniques

Fig. 8 Some important milestones and events in the 1990s

Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 14

and tools laid the foundation for the more sophisticated and automated network management
methods used today.

Security Audits:

In the 1980s, security audits were much different than they are today. Back then, computer security was not as big of a concern as it is now, and there were fewer regulations and standards in place to ensure the protection of sensitive information. Security audits in the 1980s were often performed manually and involved a review of a system's physical and logical security controls. This often included evaluating access controls, such as passwords and permissions, as well as the physical security of the computer equipment and data storage media. Due to the limited technology available at the time, security audits were typically limited to reviewing written policies and procedures, interviewing staff, and observing the actual implementation of security controls. Automated tools were limited for testing or assessment, and many security vulnerabilities went undetected. Overall, security audits in the 1980s were less comprehensive and less sophisticated than they are today, but they did lay the foundation for the development of modern security audit practices.

3d. In 1990s

In the 1990s, network security was primarily focused on protecting against unauthorized access and viruses. The methods used to achieve this included:

1. *Encryption:* Encryption was used to secure data transmitted over networks, making it more difficult for unauthorized parties to access sensitive information.
2. *Antivirus software:* Antivirus software was an essential tool for protecting networks from malicious software, such as viruses and worms, which could cause damage or disrupt operations.
3. *Access control:* Access control was used to manage and regulate who could access network resources and information. This was typically achieved using passwords, user accounts, and permission settings.

These methods were basic compared to the more sophisticated security solutions available today, but they were effective in providing a baseline level of security for networks in the 1990s.

Encryption:

In the 1990s, several encryption techniques were commonly used:

1. *Symmetric Key Algorithms:* Symmetric key algorithms, such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES), were widely used for encryption and decryption. DES was

the most used encryption standard in the 1990s but was later considered to be weak due to the increasing power of computers.

2. *Asymmetric Key Algorithms:* Asymmetric key algorithms, such as RSA, were also used for secure communication. RSA is a public-key cryptography algorithm that was developed in the 1970s and became widely used in the 1990s for secure communication and digital signatures.
3. *Hash Functions:* Hash functions, such as SHA-1, were used for ensuring the integrity of data. Hash functions generate a fixed-length digest of a message that can be used to verify the authenticity of the message.
4. *Stream Ciphers:* Stream ciphers, such as RC4, were also used for encryption in the 1990s. Stream ciphers encrypt data by generating a stream of random keystream bits and XORing them with the plaintext to produce the ciphertext.
5. *Block Ciphers:* Block ciphers, such as DES and AES, were used for encrypting fixed-length blocks of data. Block ciphers encrypt data by dividing the plaintext.

into fixed-length blocks and then encrypting each block separately.

These encryption techniques were used in a variety of applications, including secure email, virtual private networks (VPNs), and secure web communications. The widespread use of encryption in the 1990s paved the way for secure communication and commerce on the internet and helped to establish the foundation for secure online transactions that are widely used today.

Antivirus Software:

In the 1990s, antivirus software was still in its initial stages of development and deployment, but several antivirus programs were already in use. Some of the popular antivirus software used in the 1990s include:

1. *McAfee VirusScan:* McAfee VirusScan was one of the earliest antivirus programs and was first released in 1987. It became one of the most widely used antivirus software in the 1990s.
2. *Norton Antivirus:* Norton Antivirus was first released in 1990 and quickly became a popular antivirus software. It was known for its comprehensive virus detection and removal capabilities.
3. *Dr. Solomon's Anti-Virus Toolkit:* Dr. Solomon's Anti-Virus Toolkit was another popular antivirus software that was widely used in the 1990s. It was known for its ability to detect and remove a wide range of viruses, including macro viruses and boot sector viruses.
4. *Central Command Antivirus:* Central Command Antivirus was a popular antivirus software that was known for its ease of use and its ability to detect and remove viruses in real time.
5. *F-Secure Anti-Virus:* F-Secure Anti-Virus was another popular antivirus software used in the 1990s. It was known for its ability to detect and remove viruses, as well as its ability to provide real-time protection against new viruses.

applications. ACLs were often used in combination with passwords to provide a more secure form of access control.

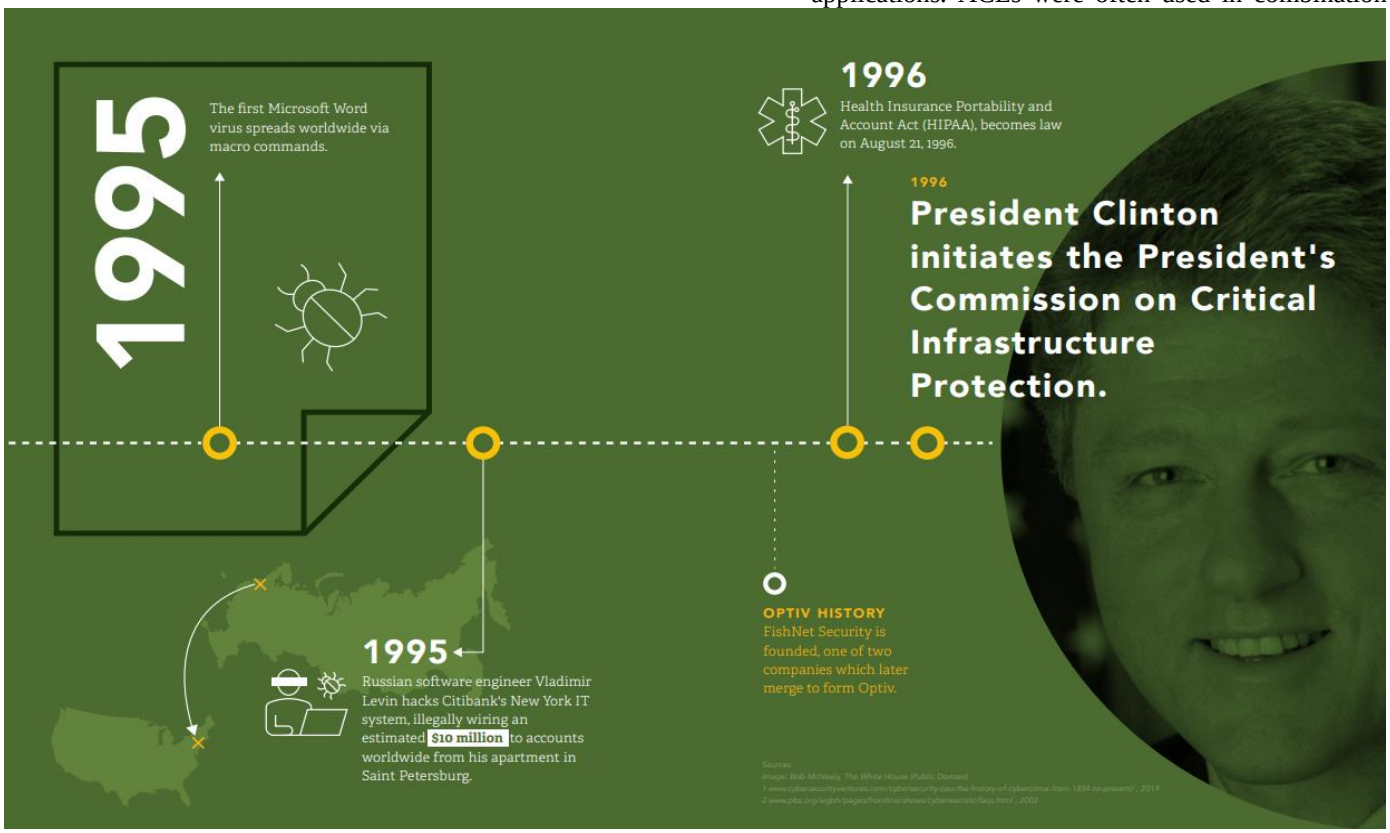


Fig. 9 Some important milestones and events in the 1990s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 15

These antivirus programs helped to protect computers from the growing threat of viruses, which were becoming increasingly prevalent as the use of personal computers and the internet grew. These early antivirus programs laid the foundation for the more sophisticated antivirus software that is widely used today to protect against the ongoing threat of malware.

Access Control:

In the 1990s, access control was primarily achieved using passwords and access control lists (ACLs). These techniques were used to secure computers, networks, and applications, and to ensure that only authorized users had access to sensitive data.

1. *Passwords:* Passwords were the most generic form of authentication in the 1990s. Users were required to enter a password to access a computer, network, or application. Passwords were typically stored in hashed form in a database, to protect against unauthorized access.
2. *Access Control Lists (ACLs):* ACLs were used to specify which users or groups of users were allowed to access specific resources, such as files, directories, and
3. *Smart Cards:* Smart cards were also used for access control in the 1990s. Smart cards are small plastic cards with integrated circuits that can store and process data. They were used for authentication by requiring users to enter a personal identification number (PIN) in addition to presenting the card.
4. *Biometric Authentication:* Biometric authentication was in its initial stages of development in the 1990s, but was beginning to be used in some applications, such as secure facilities and high-security environments. Biometric authentication uses unique biological characteristics, such as fingerprints, to verify a person's identity.

These techniques were used to ensure that only authorized users had access to sensitive data and resources and to prevent unauthorized access. While these techniques were effective in their time, they have since been replaced by more sophisticated forms of access control, such as multi-factor authentication and biometric authentication, which provide a higher level of security.

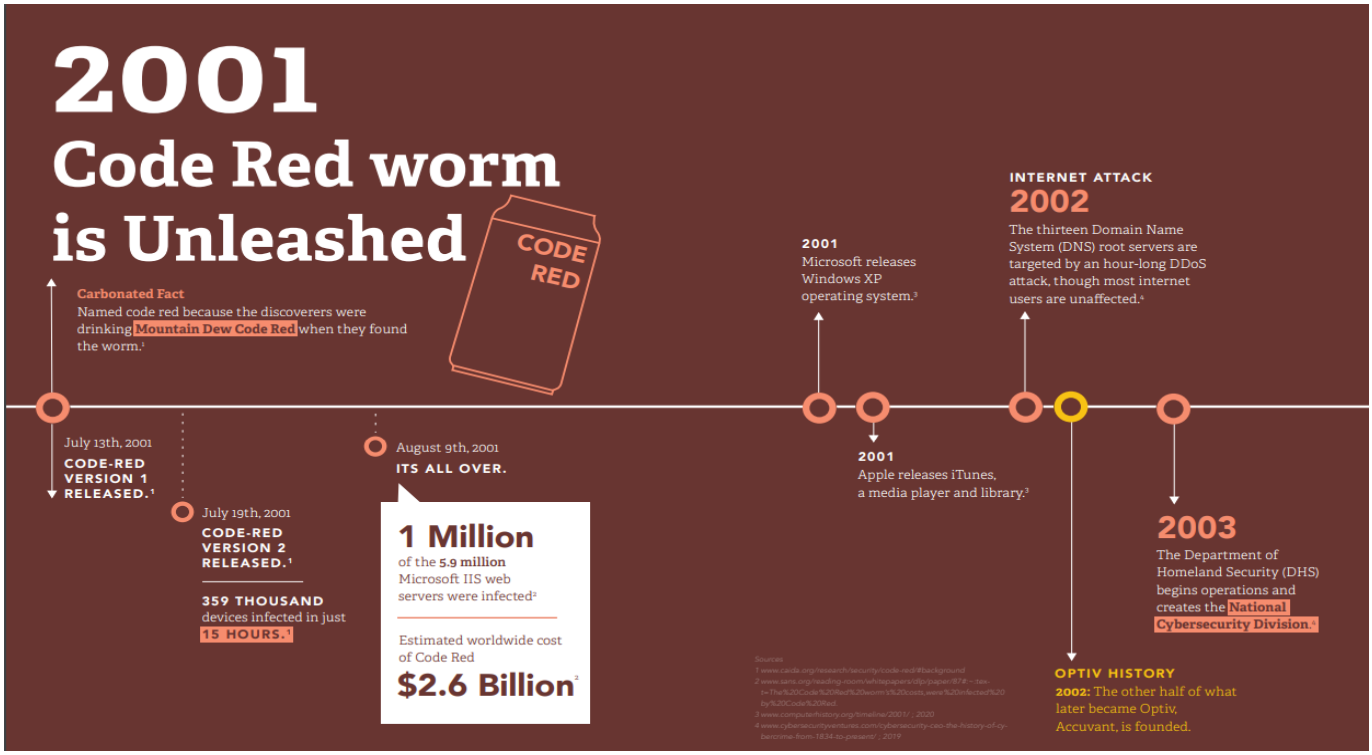


Fig. 10 Some important milestones and events in the 2000s Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 20

3e. In 2000s

In the 2000s, network security was a major concern as the use of the Internet and computer networks continued to grow rapidly. The following were some of the key trends and developments in network security during this time:

1. *Virtual Private Networks (VPNs):* VPNs became increasingly popular in the early 2000s as a means of securely connecting remote users to corporate networks. VPNs were used to encrypt network traffic so that it could not be intercepted and read by unauthorized users.
2. *Intrusion Detection Systems (IDSs):* IDSs were used to detect and respond to security threats on networks. IDSs monitored network traffic for signs of malicious activity, such as network scans or buffer overflows, and took appropriate action when such activity was detected.
3. *Patch Management:* In the early 2000s, patch management became an important part of network security, as software vendors released patches to fix security vulnerabilities in their products. Organizations were advised to install these patches promptly to protect against the exploitation of these vulnerabilities.

Overall, the early 2000s saw significant advances in network security, as organizations sought to protect their networks and data from the growing threat of cyber-attacks. These developments helped to establish the foundation for the more sophisticated security measures that are widely used today to protect networks and data from cyber threats.

VPNs:

In the 2000s, Virtual Private Networks (VPNs) emerged as a popular tool for securely connecting remote users to corporate networks. VPNs allowed organizations to extend their internal networks to remote users over the Internet while maintaining the security and privacy of the internal network.

1. *Tunnelling Protocols:* VPNs used a variety of tunneling protocols, such as Point-to-Point Tunnelling Protocol (PPTP), Layer 2 Tunnelling Protocol (L2TP), and Internet Protocol Security (IPsec), to encrypt network traffic between remote users and the internal network. This encrypted traffic was transmitted over the public Internet, making it secure against eavesdropping and tampering.
2. *Remote Access VPNs:* Remote access VPNs were widely used in the early 2000s to allow remote users to securely connect to their corporate networks over the Internet. Remote access VPNs used a combination of authentication, encryption, and authorization to ensure that only authorized users could access the internal network.
3. *Site-to-Site VPNs:* Site-to-site VPNs were also widely used in the early 2000s, to allow organizations to securely connect their internal networks across various

locations. Site-to-site VPNs used encryption to secure network traffic between sites and were often used to connect remote branch offices to the corporate headquarters.

4. *Firewall Integration:* VPNs were often integrated with firewalls, to provide an additional layer of security for remote access and site-to-site connections. Firewalls were used to restrict incoming and outgoing network traffic based on a set of predefined rules and to block unauthorized access and malicious attacks.

Overall, VPNs in the early 2000s played a key role in enabling organizations to securely extend their internal networks to remote users, while maintaining the security and privacy of the internal network. VPNs were widely used by organizations of all sizes to support remote work and connect remote sites and continue to be a valuable tool for network security today.

Fig. 11 Some important milestones and events in the 2000s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 24

IDSs:

In the 2000s, Intrusion Detection Systems (IDSs) emerged as a valuable tool for detecting and responding to security threats on computer networks. IDSs were used to monitor network traffic for signs of malicious activity, such as network scans, buffer overflows, and unauthorized access, and to alert network administrators when such activity was detected.

1. *Signature-based Detection:* One of the most widely used techniques for intrusion detection in the early 2000s was signature-based detection. Signature-based IDSs used a database of known malicious activity, such as viruses and worms, to detect and alert potential threats.
2. *Anomaly-based Detection:* Anomaly-based IDSs were used to detect deviations from normal network behavior that might indicate the presence of a security threat. Anomaly-based IDSs monitored network traffic for unusual patterns, such as high volumes of traffic from a sole source, and raised alerts when such patterns were detected.
3. *Network-based IDSs:* Network-based IDSs were used to monitor network traffic in real-time, looking for signs of malicious activity, such as unauthorized access, network scans, and buffer overflows. Network-based IDSs were typically deployed at key points in the network, such as at network gateways or firewalls, to monitor all incoming and outgoing network traffic.
4. *Host-based IDSs:* Host-based IDSs were used to monitor the activity on individual computers or servers, looking for signs of malicious activity, such as unauthorized access, file modifications, and system calls. Host-based IDSs were typically deployed on

critical systems, such as servers and databases, to provide an additional layer of protection for these systems.

Overall, IDSs in the early 2000s played a key role in protecting computer networks from security threats, by detecting and alerting potential threats and providing network administrators with the information they needed to respond to security incidents. IDSs continue to be valuable tool for network security today and have evolved to incorporate more sophisticated techniques, such as machine learning, for improved threat detection and response.

Fig. 12 Some important milestones and events in the 2000s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 25

Patch Management:

In the 2000s, patch management was a vital component of network security. Patch management refers to the process of identifying, testing, and applying software updates to address known security vulnerabilities in software and operating systems. The following were some of the techniques used for patch management in network security in the 2000s:

1. *Vulnerability Scanning:* Vulnerability scanning tools were used to identify missing patches and security vulnerabilities in software and operating systems. Vulnerability scanning tools would regularly scan the network for vulnerable systems and generate reports that highlighted which systems required patches.
2. *Centralized Management:* To streamline the patch management process, organizations would use centralized management tools to manage and deploy patches across their networks. These tools would download patches from the vendor's website, evaluate the patches for compatibility, and then deploy the patches to the appropriate systems.
3. *Testing and Deployment:* Before deploying patches to production systems, organizations would perform thorough testing to ensure that the patches would not cause any disruption to normal operations. Once the patches had been evaluated and approved, they would be deployed to the appropriate systems.
4. *Scheduling:* To ensure that patches were applied promptly, organizations would schedule regular patch management cycles to coincide with the release of new patches. This would ensure that systems were kept up to date with the latest security updates.
5. *Automation:* To reduce the time and effort required to manage patches, organizations would use automation tools to automate the patch management process. Automation tools would automate the process of downloading, testing, and deploying patches, freeing up IT staff to focus on other tasks.

Overall, patch management was an important part of network security in the 2000s and was used to address known security vulnerabilities in software and operating systems. Effective patch management helped organizations to reduce the risk of security incidents and ensure the security and integrity of their

networks.

3f. In 2010s

The 2010s saw several advancements and improvements in network security compared to the 2000s. Some of the major things and methodologies used in network security during the 2010s include:

1. *Next-Generation Firewalls:* Next-generation firewalls (NGFWs) are a more advanced form of traditional firewalls. NGFWs offer greater application control, user identification, and threat intelligence capabilities, which help to detect and prevent a wide range of cyber threats.
2. *Intrusion Prevention Systems:* Intrusion prevention systems (IPS) are network security appliances that monitor network traffic for potential malicious activities or policy violations. They analyze packets and traffic flows for suspicious patterns, which can be used to prevent attacks before they occur.
3. *Threat Intelligence:* Threat intelligence involves the collection, analysis, and dissemination of information about emerging and current cyber threats. This helps organizations stay ahead of the game and prevent cyber-attacks before they happen.
4. *Cloud-Based Security:* Cloud-based security solutions have become increasingly popular in recent years. Cloud-based security solutions are more scalable, flexible, and cost-effective than traditional on-premises security solutions.
5. *Zero-Trust Security:* Zero-trust security is a security model that assumes that all users and devices, whether inside or outside of the network, are untrusted. It requires strict authentication and authorization policies, as well as continuous monitoring and analysis of user and device behavior.

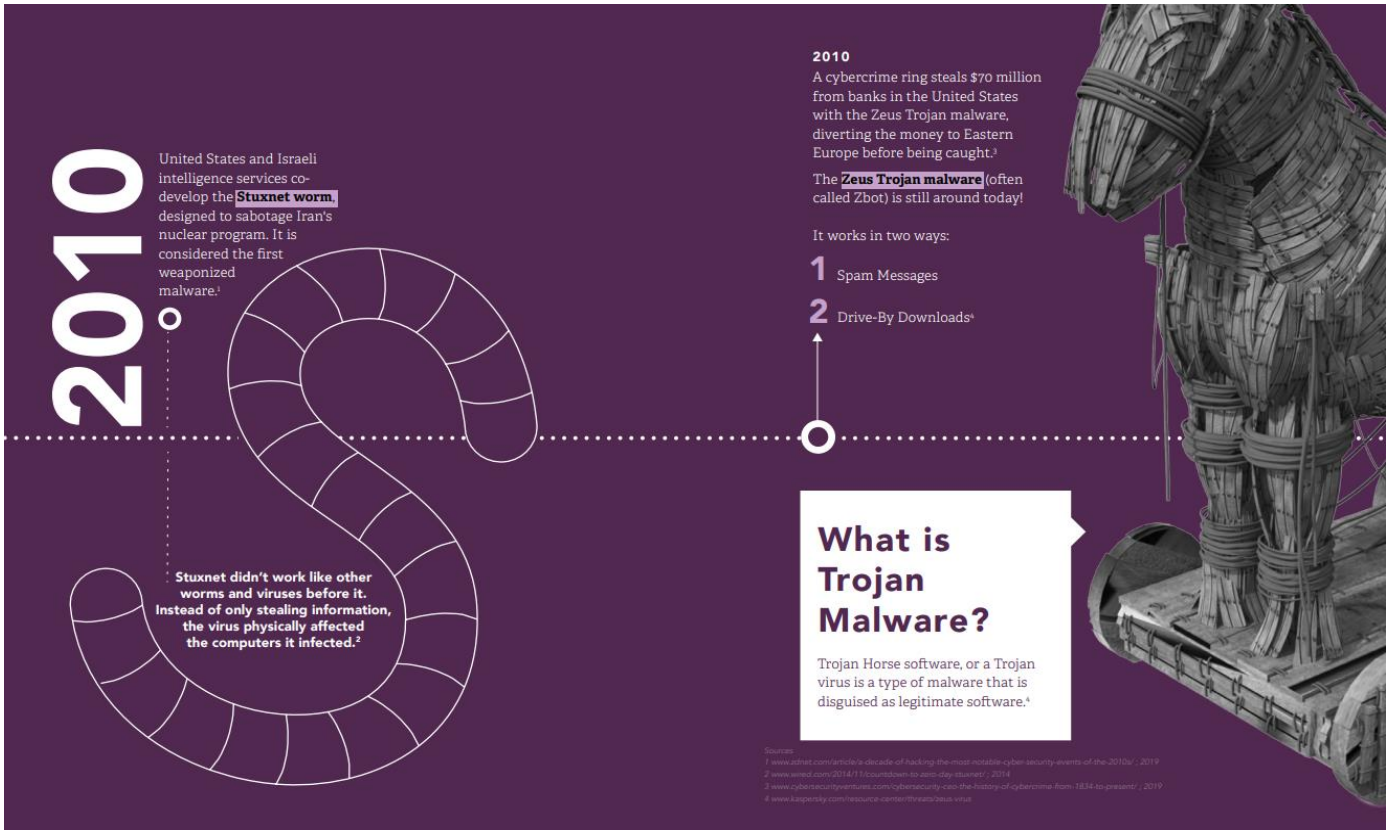


Fig. 13 Some important milestones and events in the 2010s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 2

Cloud-Based Security:

Cloud-based security in the 2010s was a new concept, and it was still evolving rapidly. However, there were several significant developments and advancements during this period that helped to make cloud-based security more robust and effective. One of the key developments during this time was the emergence of cloud-based security platforms that provided a range of security services, such as firewalls, intrusion detection and prevention, and threat intelligence. These platforms

allowed organizations to deploy security solutions quickly and easily, without the need for on-premises hardware or software. Another important advancement in cloud-based security during the 2010s was the introduction of Security-as-a-Service (SECaaS) offerings. SECaaS solutions provided security services, such as identity and access management, vulnerability scanning, and security information and event management (SIEM), on a subscription basis, reducing the cost and complexity of deploying and managing security solutions. Cloud-based security also benefited from the growing use of virtualization technology, which allowed security services to be delivered as virtual appliances that could be deployed in the cloud. This allowed organizations to deploy security solutions quickly and easily, without the need for physical hardware.

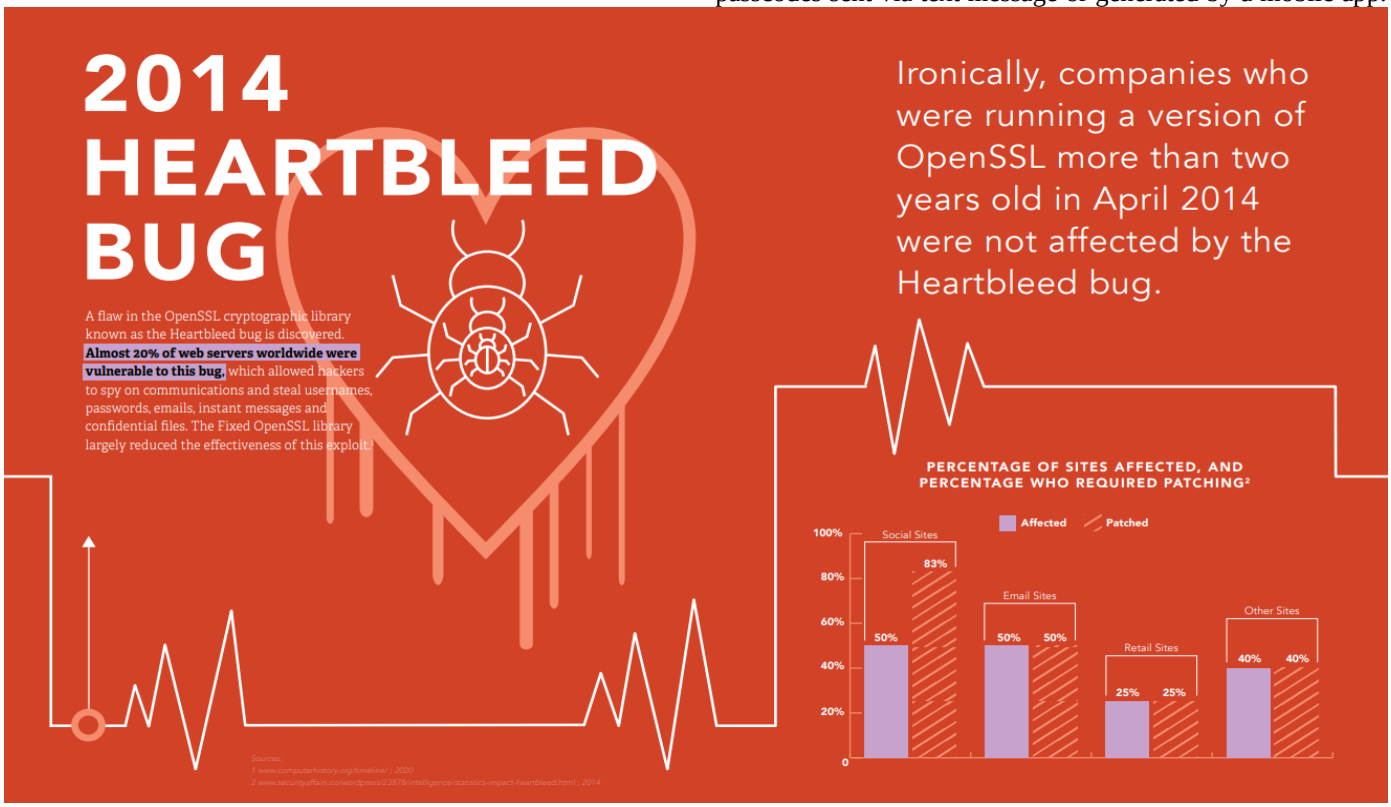


Fig. 14 Some important milestones and events in the 2010s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 34

Zero-Trust Security:

Zero Trust security was a new concept in the 2010s, but it was gaining popularity as an effective approach to network security. The idea behind Zero Trust security is to treat all network traffic and users as potentially hostile and to verify each request for access to resources, regardless of the user's location or device. One of the key concepts of Zero Trust security is the principle of least privilege, which means that users are only given access to the resources they need to perform their job functions. This helps to limit the potential damage that can be caused by a compromised user account.

In the 2010s, Zero Trust security was typically implemented using a combination of technologies, including identity and access management (IAM) solutions, multi-factor authentication (MFA), and network segmentation. IAM solutions were used to manage user identities and control access to resources. These solutions allowed organizations to define granular access policies based on the user's role, location, and other attributes, and to enforce those policies consistently across the network. MFA was used to provide an additional layer of authentication beyond simple username and password credentials. This could include biometric authentication, such as fingerprint or facial recognition, or the use of one-time passcodes sent via text message or generated by a mobile app.

Network segmentation was used to create isolated network zones for diverse types of users and resources. This helped to prevent lateral movement within the network by isolating

compromised devices or user accounts.

NGFWs:

Next-generation firewalls (NGFWs) were a significant advancement in network security during the 2010s. These firewalls were designed to provide more advanced and comprehensive security features than traditional firewalls.

In the 2010s, NGFWs typically offered the following features:

1. *Application awareness:* NGFWs could identify and control applications at a granular level, including

specific functions within an application. This allowed organizations to enforce application usage policies and prevent the use of unauthorized applications.

2. *User identification:* NGFWs could identify users by their login credentials or by analyzing their network behavior. This allowed organizations to enforce access policies based on user identity, such as restricting access to sensitive data to specific groups of users.
3. *Threat intelligence:* NGFWs could use threat intelligence feeds to detect, and block known malicious IP addresses, domains, and URLs. They could also use machine learning algorithms to analyze network traffic patterns and detect anomalies that could indicate the presence of a new or unknown threat.
4. *Intrusion prevention:* NGFWs could block known attack vectors, such as SQL injection and cross-site scripting, and use behavioral analysis to detect and prevent new and unknown attacks.
5. *Secure sockets layer (SSL) decryption:* NGFWs could decrypt SSL traffic to inspect it for threats, even if the traffic was encrypted.

Overall, NGFWs were a significant improvement over traditional firewalls, which typically focused on packet filtering and port blocking. NGFWs provided a more comprehensive security posture by incorporating application awareness, user identification, threat intelligence, and intrusion prevention. By offering greater visibility and control over network traffic, NGFWs were better able to detect and prevent a wide range of cyber threats in the 2010s.

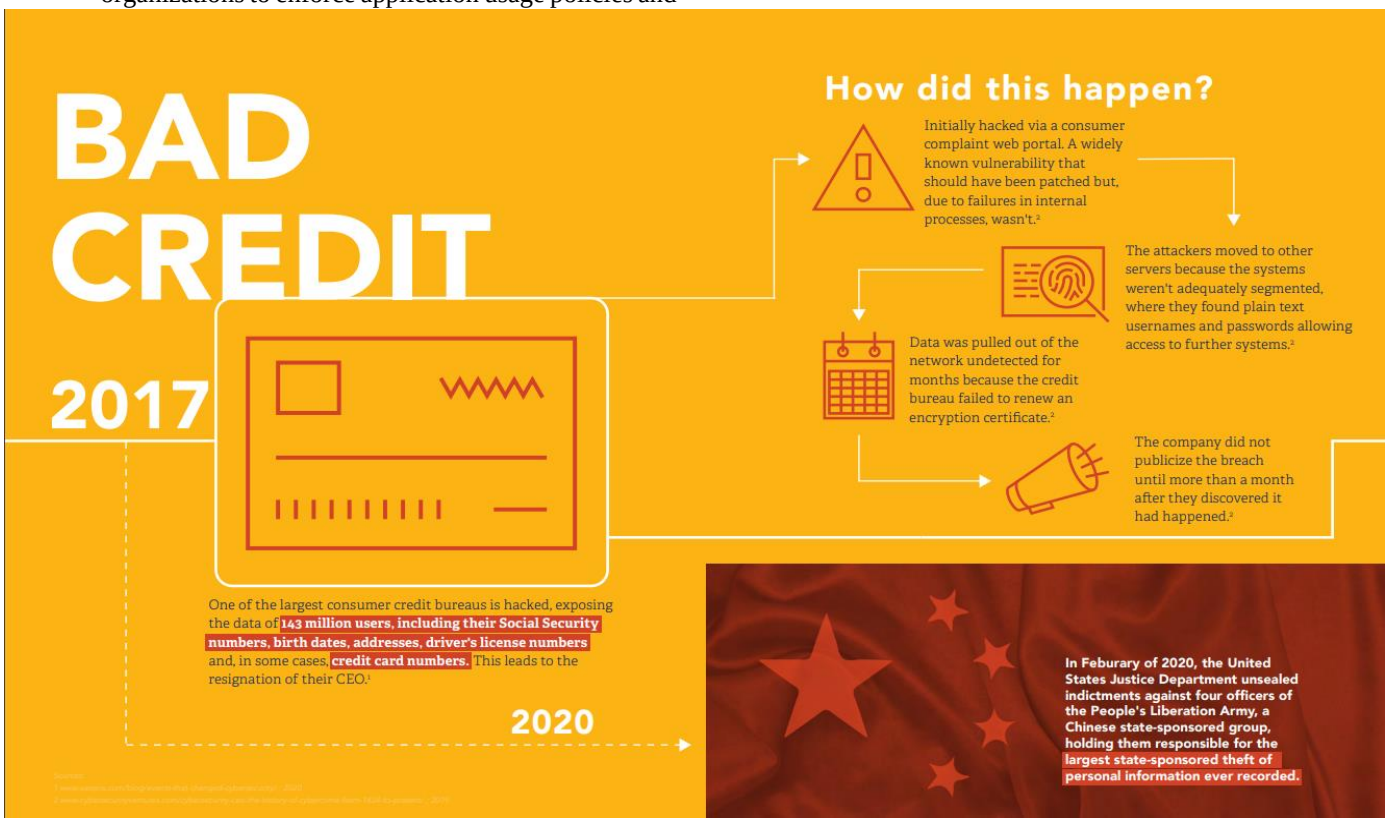


Fig. 15 Some important milestones and events in the 2010s
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 38

3g. 2020 to Present.

Since the COVID-19 pandemic, there have been some notable changes and new inventions in network security that are different from what was being used before 2020. Some of the most notable ones include:

1. *Zero Trust Network Access (ZTNA):* ZTNA is a variation of Zero Trust security that specifically focuses on providing secure remote access to applications and resources. This approach uses a software-defined perimeter to create a secure tunnel between the user and the application, reducing the risk of cyber-attacks.
2. *Secure Access Service Edge (SASE):* SASE is a cloud-based security model that combines network security and wide-area networking (WAN) technologies into a single solution. SASE solutions provide

comprehensive security features, including secure web gateways, cloud access security brokers (CASB), and zero trust network access (ZTNA).

3. *Extended Detection and Response (XDR):* XDR is an evolution of endpoint detection and response (EDR) that provides comprehensive visibility across multiple endpoints and data sources. XDR solutions use advanced analytics and machine learning to detect and respond to threats across the entire network.
4. *DevSecOps:* DevSecOps is an approach to software. development that incorporates security into the development process from the beginning. This approach helps to identify and mitigate security risks earlier in the development cycle, reducing the risk of vulnerabilities and exploits.
5. *Security Orchestration, Automation, and Response (SOAR):* SOAR is an approach to incident response that uses automation and orchestration to improve the speed and efficiency of incident response. This approach helps to reduce the time to detection and response, minimizing the impact of security incidents.

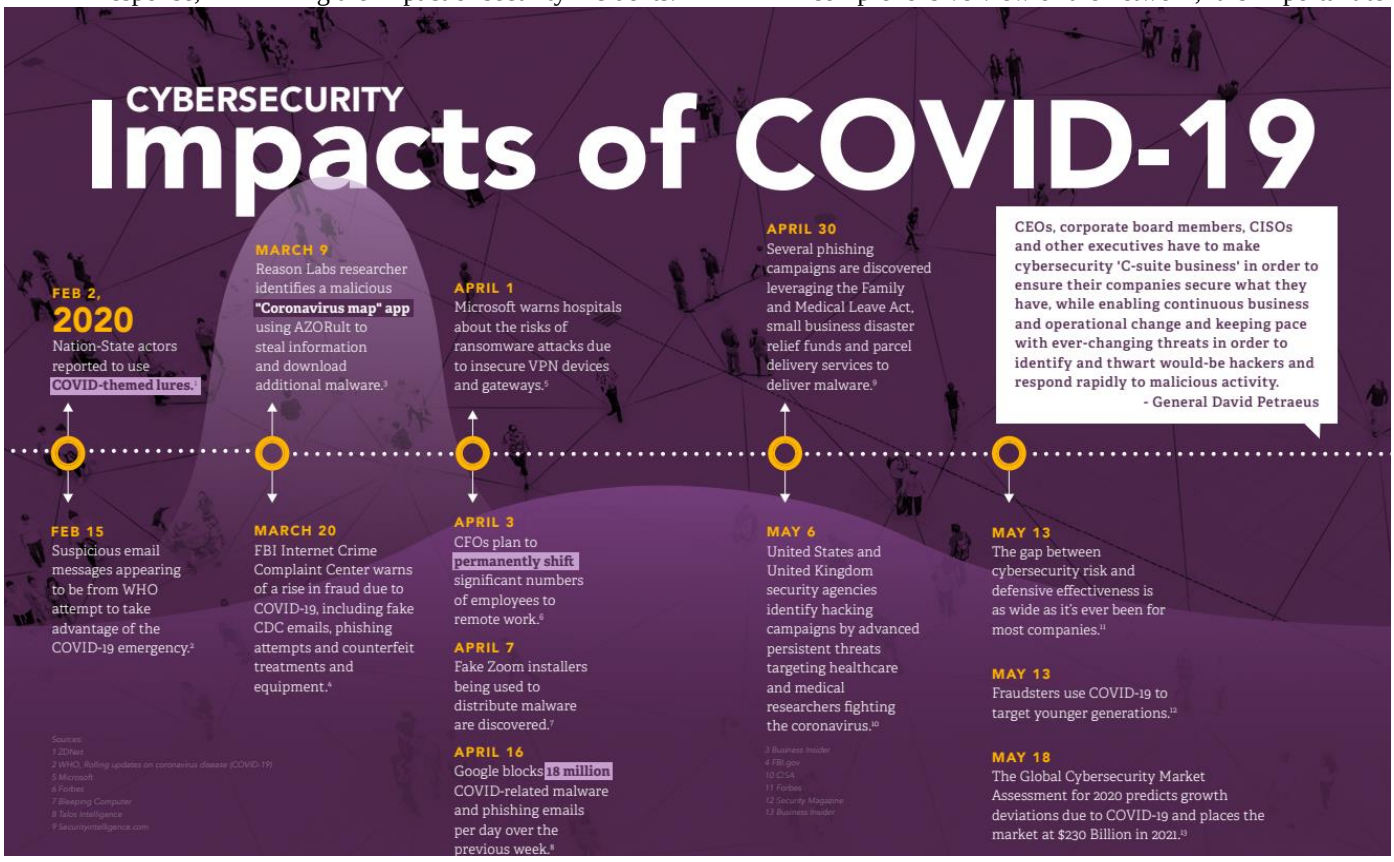


Fig. 16 Some recent important milestones and events
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 42

XDR:

Extended Detection and Response (XDR) solutions are created by integrating multiple security technologies and data sources into a single platform. This typically involves integrating endpoint detection and response (EDR) solutions with other security technologies, such as network security, cloud security, and email security. XDR solutions use advanced analytics and machine learning algorithms to analyze data from all these sources and to identify and respond to threats across the entire network. The goal is to provide security teams with a unified view of the security posture of their organization and to enable them to respond more quickly and effectively to security incidents. XDR solutions are typically cloud-based, which enables them to scale easily and be accessible from anywhere. They can be deployed as a managed service, where the XDR vendor provides security monitoring and incident response services, or as a self-managed solution, where the organization manages the solution in-house.

When using XDR, organizations typically follow a set of best practices to ensure that the solution is effective and efficient. These include:

1. Integrating all relevant data sources: To get a comprehensive view of the network, it is important to integrate all relevant data sources into the XDR solution. This includes endpoint, network, cloud, and email data.
2. Configuring rules and alerts: XDR solutions generate

many alerts, so it is important to configure rules and alerts that are tailored to the organization's specific security needs. This can help to reduce false positives and to prioritize alerts that require immediate attention.

3. Automating incident response: XDR solutions can automate incident response processes, such as containment and remediation. This can help to reduce the time required to respond to security incidents and to minimize the impact of the incident.
4. Regularly reviewing and tuning the solution: XDR solutions are not set-and-forget technologies, and they require regular review and tuning to ensure that they remain effective and efficient. This includes reviewing alerts, rules, and policies, and adjusting as needed.

Overall, XDR represents an important evolution in cybersecurity, as it provides a more comprehensive and integrated approach to threat detection and response. As organizations continue to adopt cloud-based infrastructure and distributed workforces, XDR will become increasingly important for protecting against advanced cyber threats.

DevSecOps:

DevSecOps is a methodology that emphasizes the integration of security into the software development lifecycle (SDLC) by integrating security testing and automation into the DevOps process. It is designed to improve the overall security of software products by making security a priority throughout the SDLC, rather than treating it as an afterthought. DevSecOps is created by integrating security testing and automation tools into the DevOps toolchain. This involves automating security testing and vulnerability scanning, as well as integrating security into the code review process. Developers are trained to identify and remediate security vulnerabilities early in the SDLC, and security teams work closely with development and operations teams to ensure that security is incorporated into every stage of the process. The goal of DevSecOps is to enable organizations to deliver secure software products more quickly and efficiently. By integrating security into the SDLC, organizations can reduce the time and cost required to remediate security issues and can improve the overall quality of their software products.

DevSecOps is used in a variety of ways by organizations. Some organizations may have dedicated DevSecOps teams that work closely with development and operations teams to integrate security into the SDLC. Others may integrate security into their existing DevOps processes, using security tools and automation to evaluate code and identify vulnerabilities.

Fig. 17 Some recent important milestones and events
Link Ref - https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf page 47

To use DevSecOps effectively, organizations should follow a set of best practices, including:

1. Integrating security testing and automation into the DevOps toolchain: This involves identifying the appropriate security tools and integrating them into the DevOps process.
2. Incorporating security requirements into the SDLC: This involves identifying security requirements and incorporating them into the SDLC, including requirements gathering, design, development, testing, and deployment.
3. Training developers and security teams: Developers should be trained to identify and remediate security vulnerabilities, while security teams should be trained to work closely with development and operations teams to integrate security into the SDLC.
4. Continuous monitoring and improvement: DevSecOps are a continuous process, and organizations should continuously monitor and improve their security posture to ensure that they remain protected against the latest threats.

Overall, DevSecOps is an important methodology for improving the security of software products. By integrating security into the SDLC, organizations can improve the overall quality and security of their software products and can deliver them more quickly and efficiently.

SOAR:

SOAR (Security Orchestration, Automation, and Response) is a security technology platform that allows organizations to automate and orchestrate their security operations. SOAR combines security orchestration, automation, and response into a single platform to provide security teams with the tools they need to respond quickly and efficiently to security incidents.

SOAR is created by integrating security tools and technologies into a single platform. This involves integrating security incident and event management (SIEM) systems, endpoint detection, and response (EDR) systems, threat intelligence feeds, vulnerability scanners, and other security technologies into a single platform. SOAR solutions use advanced analytics and machine learning algorithms to analyze data from all these sources and to identify and respond to threats across the entire network. The goal is to provide security teams with a unified view of the security posture of their organization and to enable them to respond more quickly and effectively to security incidents. SOAR solutions are typically cloud-based, which enables them to scale easily and be accessible from anywhere. They can be deployed as a managed service, where the SOAR vendor provides security monitoring and incident response services, or as a self-managed solution, where the organization manages the solution in-house.

To use SOAR effectively, organizations should follow a set of best practices, including:

1. Identifying key security use cases: Organizations should identify the key security use cases that they need to address, such as phishing attacks, ransomware, or insider threats.
2. Integrating all relevant data sources: To get a comprehensive view of the network, it is important to integrate all relevant data sources into the SOAR solution. This includes endpoint, network, cloud, and email data.
3. Configuring rules and workflows: SOAR solutions use workflows to automate incident response processes, such as containment and remediation. It is important to configure rules and workflows that are tailored to the organization's specific security needs.
4. Automating incident response: SOAR solutions can automate incident response processes, such as containment and remediation. This can help to reduce the time required to respond to security incidents and to minimize the impact of the incident.
5. Regularly reviewing and tuning the solution: SOAR solutions are not set-and-forget technologies, and they require regular review and tuning to ensure that they remain effective and efficient. This includes reviewing workflows, rules, and policies, and adjusting as needed.

Overall, SOAR represents an important evolution in cybersecurity, as it provides a more comprehensive and integrated approach to threat detection and response. As organizations continue to face increasingly sophisticated cyber threats, SOAR will become increasingly important for protecting against advanced attacks.

5. FUTURE TRENDS IN SECURITY

What is going to drive Internet security is the set of applications more than anything else. The future will be that security is like an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system. The trend toward biometrics could have taken place a while ago, but it is not being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

6. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software-based, but many common hardware devices are used. The current development in network security is not very impressive. Originally it was assumed that with the importance

of the network security field, innovative approaches to security, both hardware and software, would be actively researched. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

7. REFERENCES

- https://www.optiv.com/sites/default/files/2022-04/history-book-2022.pdf
- "Cybersecurity and Cyberwar: What Everyone Needs to Know" by P.W. Singer and Allan Friedman
- "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography" by Simon Singh
- "A brief history of network security" by Robyn Weisman. Link: https://www.techradar.com/news/a-brief-history-of-network-security
- "A Brief History of Cybersecurity" by Mestre. Link: https://www.researchgate.net/publication/318012326_A_Brief_History_of_Cybersecurity
- "A Brief History of Cybersecurity" by Richard Stiennon. Link: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/a-brief-history-of-cybersecurity/
- "The history of firewall technology: A paper" by Jane Link: https://repository.uwl.ac.uk/id/eprint/1442/
- "A brief history of Internet security" by W. Stallings. Link: https://www.sciencedirect.com/science/article/pii/S1364815204000191

8. ACKNOWLEDGMENT

We would like to express our deep gratitude to our research supervisor, Mr. Aditya Gupta, for his invaluable guidance, insightful comments, and unwavering support throughout the research process. His extensive knowledge and expertise in the field have been a constant source of inspiration to us.

We are also grateful to the participants of this study who generously gave their time and shared their experiences with us. Their willingness to participate and their thoughtful responses have been critical to the success of this research.

We would like to extend our appreciation to our colleagues who provided valuable feedback and support throughout the research process. Their insights and suggestions have greatly contributed to the quality of this research.

We would also like to acknowledge the support provided by Manipal University Jaipur in terms of facilities, and resources. Without this support, this research would not have been possible.

Lastly, we would like to thank our families and friends for their unwavering support, patience, and encouragement throughout the research process.

Deepanshu Jain born 14th March 2002 in Gwalior, Madhya Pradesh, India is an Undergraduate Engineering student currently pursuing computer science at Manipal University Jaipur.

Ankur Sheth born 8th May 2002 in Pune, Maharashtra, India is an Undergraduate Engineering student currently pursuing computer science at Manipal University Jaipur.