International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# Comprehensive Research on Cyber - Attacks and Cyber Security

**Sonam Khatri**

## 1. Introduction

Computer networks and information technology solutions have become more and more important in our society, economy, and essential infrastructures. As our reliance on information technology grows, cyber attacks are becoming more compelling and potentially disastrous. Cyber attacks cost the US$214 billion every year, as per a Symantec cybercrime report issued in April 2020. If the time was spent by businesses seeking to retrieve from cyber attacks is considered in, the overall cost of cyber attacks rises to a stunning $585 billion. The proportion of people who have already been harmed by cyber - attacks is certainly on the rise. As per a Symantec survey of 2.5 million people in 34 countries, 32 per cent said they had been the target of cyber assault at a certain point in life. Thus according Symantec, 24 people are victims of a cybercrime per second.

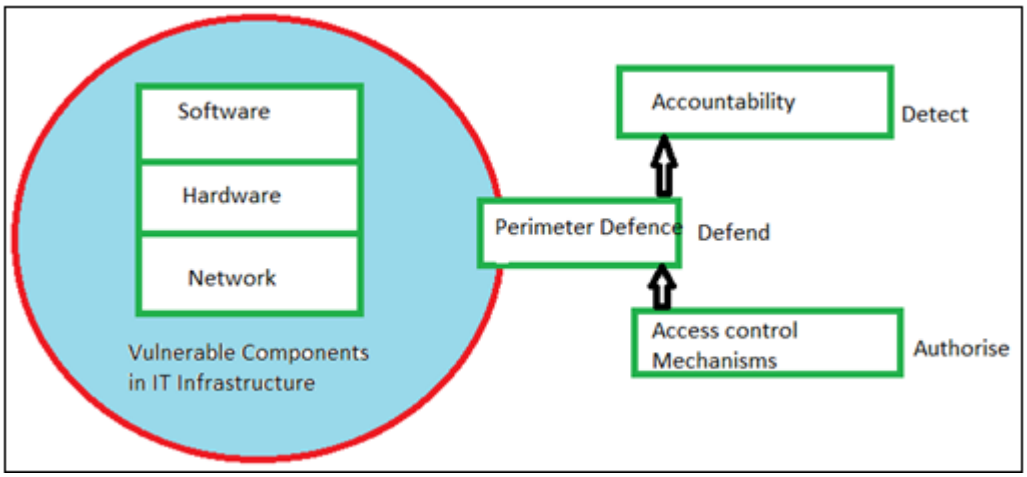
So how are cyber - attacks upon that increase? Since cyber attacks are far less cheap, more convenient, and less risky than physical attacks. Apart from a computer and an Internet service, cyber criminals only needed a few things. They aren't limited by geography or distance. Due to the obvious invisible nature of online, they are difficult to identify and prosecute. Given how compelling cyber attacks over information technology systems are, it's likely that the volume and cybercriminals will keep rising.

Understanding the challenges surrounding various cyber attacks and developing defense methods that preserve the confidentiality, integrity, and accessibility of any information and digital technologies are all part of cybersecurity.

Malware may spread through embedded devices and computational logic in devices and equipment. Malware can be introduced at any time throughout the system's life cycle. Malware victims might include end user computers, servers, network equipment (such as routers and switches), and process control systems like Supervisory Control and Data Acquisition (SCADA). The rapid prevalence and complexity of malware is a major source of concern on the Internet nowadays.

Malware assaults have traditionally occurred at a single point of entry among hardware, software, or network components, exploiting known design and implementation weaknesses at each layer. Rather than safeguarding individual assets, the perimeter defense concept has mostly been employed to create a barrier around all internal resources. Keep everything inside safe from intruders from the outside. The bulk of perimeter defense measures rely on firewall and anti - virus software installed within intrusion prevention/detection systems. Any communication coming in from the outside is captured and inspected to verify that no virus has infiltrated the internal network. Because securing a single perimeter is significantly easier and appears to be less expensive than securing a big volume of applications or a large number of internal networks, this perimeter defence concept has gained widespread support.

Accountability is added to perimeter defiance and access control to identify and penalize any misbehaviors, as shown in Fig.1. However, as malware evolves and becomes more sophisticated, the combined efforts of perimeter defensive strategies have been shown to be more unsuccessful. At the hardware, software, and network layers of an existing information system, we discuss the most prevalent exploitations in detail. The advantages and disadvantages of the most typical protection methods utilized in these tiers are then discussed.



To escape detection, malware changes throughout time, capitalizing on new tactics and exploiting holes in newer technology. In this paper, we explain a variety of novel malware attack patterns seen in developing technology. We chose a few developing technologies to illustrate since they have impacted the way we live our lives. Social media, cloud computing, smart phone technology, and vital infrastructure are examples of these.

### 1.1 Malware as attack tool

Malware was formerly merely produced as an experiment to illustrate security flaws or, in certain situations, to demonstrate technological prowess. Malware is now mostly used to steal sensitive personal, financial, or corporate data for the advantage of others. Malware is frequently used to attack government or business websites in order to obtain sensitive information or disrupt operations. In other circumstances, malware is used to steal personal information such as social security numbers or credit card data from victims. Since the widespread availability of cheaper and quicker broadband Internet connection, malware has increasingly been intended not only for information stealth but also for profit.

APWG recorded 1, 025, 968 total phishing assaults in the first quarter of 2022. This was the worst phishing quarter in APWG's history, with the quarterly total exceeding one million for the first time.

Although most industries reported a decline in the total number of ransomware attacks, the Financial Services industry saw a 35 percent spike in assaults in 1Q2022. Credential theft phishing attacks against corporate users increased by 7%. Corporate executive impersonation on social media has become a growing commercial concern. With 23.6 percent of all phishing assaults in Q1, the banking sector was the most commonly targeted. The number of attacks against SaaS and webmail providers has remained high. The percentage of phishing assaults aimed at bitcoin targets has risen to 6.6 percent.

### 1.2 Exploiting existing vulnerabilities

Once malware has been installed on a victim's system, cyber criminals can use a variety of existing vulnerabilities in the victim's system to enhance their illegal operations. The most often exploited security holes in hardware, software, and network systems are examined. Following that, there will be a discussion of present and proposed attempts to ameliorate the harmful effects of the exploitations.

Following that, there will be a discussion of present and proposed attempts to ameliorate the harmful effects of the exploitations. Figure shows an overview of common assaults at the hardware, software, and network levels, as well as instances of responses.

| | Hardware | Software | Network |
|---|---|---|---|
| Common attacks | • Hardware Trojan<br>• Illegal clones<br>• Side channel attacks (i.e. snooping hardware signals) | • Software programming bugs (e.g. memory management, user input validation, race conditions, user access privileges, etc.)<br>• Software design bugs<br>• Deployment errors | • Networking protocol attacks<br>• Network monitoring and sniffing |
| Examples of countermeasures | • Tamper-Resistant Hardware (e.g. TPM)<br>• Trusted Computing Base (TCB)<br>• Hardware watermarking<br>• Hardware obfuscation | • Secure coding practice (e.g. type checking, runtime error, program transformation, etc.)<br>• Code obfuscation<br>• Secure design and development<br>• Formal methods | • Firewall<br>• Intrusion prevention and detection<br>• Virtual Private Network (VPN)<br>• Encryption |

### 1.3 Hardware

Hardware is the most privileged element in a computing system, with the most capacity to modify it. If the hardware is hacked, this level has the ability to allow attackers a lot of freedom and capacity to undertake harmful security assaults. Unlike software - based assaults, which have a plethora of security updates, intrusion detection tools, and anti - virus scanners to detect malicious attacks on a regular basis, many hardware - based attacks are capable of evading detection. Hardware - based assaults have been claimed to be on the rise, taking advantage of the absence of tools that assist hardware detection. Among the several sorts of hardware abuse, hardware Trojan is the most heinous and widespread. Hardware Trojans are malicious modifications to electronic equipment, such as Integrity Circuits (IC) in the hardware, that are done invisibly. Hardware Trojans come in a number of degrees, each with its own set of negative consequences.

### 1.4 Software defects

An error, flaw, mistake, or problem in a computer program such as the operating system, external I/O interface drivers, and applications is referred to as a software bug. Cyber assaults take use of software defects to force systems to act in unexpected ways that deviate from their original design. Today, the bulk of cyber assaults are still carried out by exploiting software vulnerabilities caused by bugs and design defects in software. When particular elements of the software stack and interface are abused, this is known as software - based exploitation. Exploiting program defects in memory, user input validation, race situations, and user access rights are the most prevalent software vulnerabilities. Attackers use memory safety breaches to change the contents of a memory location.

### 1.5 Network infrastructure and protocol vulnerabilities

The early network protocol was designed to serve an altogether different environment than we have now on a much smaller scale, and it frequently fails in many of the scenarios in which it is now employed. When both system administrators and users have inadequate awareness of the networking architecture, flaws in network protocols become more problematic.

Exploiting the constraints of the generally used network technologies Internet Protocol (IP), Transmission Control Protocol (TCP), or Domain Name System (DNS) is one of the most prevalent network assaults [14]. The IP protocol is the network layer's primary protocol. It contains the data required for packet routing between routers and computers in the network. The original IP protocol lacked a way for verifying the integrity and privacy of data being sent. This allowed data to be intercepted or modified while being sent between two devices via an unknown network. IPSec, a protocol for encrypting IP communication, was created to address this issue. For many years, IPSec has been one of the most widely used technologies for establishing a virtual private network (VPN), which establishes a secure connection between a distant computer and an Internet - based trustworthy network (i. e., company intranet). TCP stands on top of IP to ensure that packets are sent in a dependable (i. e., retransmitting missing packets) and orderly manner. SSL was created to enable end - to - end security between two computers through the transmission control protocol, rather than only layer - based protection (TCP). SSL/TLS is frequently used in conjunction with http to create https for secure Web pages. DNS stands for domain name server, and it is the mechanism that converts human - readable host names into 32 - bit Internet protocol (IP) addresses. When a user types in a URL, it acts as a directory book for the Internet, informing routers of which IP address to send packets to. An attacker may be able to transmit malicious DNS messages to impersonate an Internet server since DNS responses are not verified. The availability of DNS is another key problem. DNS has been the subject of various Denial - of - Service (DoS) assaults since a successful strike on it would cause severe communication disruption on the Internet. Cryptography is a vital technique for protecting data transmitted between users by encrypting it and allowing only those with the necessary keys to decipher it. Cryptography is the most widely utilized method of data protection.

## 2. Discussion

Rather than focusing on each layer, bundled security protection techniques that protect everything inside from outside attacks have been adopted in the traditional approach, despite the fact that many separate techniques and proposals exist to address vulnerabilities in the hardware, software, and network layers. To protect the company's network from any potential outside incursion, the vast majority of firms use a perimeter defense security approach. This strategy focuses on "layered defense" or "defense in depth" tactics, in which essential internal IT assets, such as servers and mission - critical data, are fortified with walls and fortifications. Firewalls and intrusion detection systems are common perimeter protection technology (IDS). To secure internal assets, the firewall has been the most extensively utilized technology. Its main goal is to manage incoming and outgoing network traffic by examining data packets and deciding whether or not they should be let through based on a set of rules. A firewall can be installed at several levels of the network infrastructure. Network layer firewalls, also known as packet filters, are network layer firewalls that restrict packets from passing through unless they meet the predefined rule set (i. e., configurations) provided by network administrators. Despite the fact that many current firewalls are more sophisticated, network layer firewalls cannot filter unwanted traffic that uses valid IP addresses and ports, such as malware payload. The application layer firewall monitors and possibly blocks input, output, or system service requests that do not comply with the network layer firewall's established policy. . A proxy server can behave as a firewall by acting like an application and responding to input packets (for example, connection requests) while blocking others. Tampering with an internal system is more difficult with both application layer firewalls and proxies. However, as attackers' capabilities and sophistication have grown, they've developed increasingly complicated attack methods for sending malicious packets to a target network. Intruders may, for example, take control of a publicly accessible system and use it as a proxy for their own objectives. The attacker produces packets with a forged IP address using the intercepted proxy in order to obscure the sender's identity or impersonate another computer machine.

### 2.1 Emerging threats

Cyber assaults against cyberspace change with time, taking use of new techniques. Most of the time, cyber thieves would change existing malware signatures in order to take advantage of holes in new technology. In other circumstances, they just investigate the specific qualities of new technology in order to uncover gaps via which malware might be injected. Cyber thieves take use of new Internet technologies that have millions or billions of active users to reach out to a large number of victims fast and efficiently. We use social media, cloud computing, smartphone technology, and critical infrastructure as illustrative examples to examine the vulnerabilities that these technologies pose.

### 2.2 Future research direction

With the rapid expansion of Internet access and the innovation of Internet - enabled gadgets, a rising number of people are using the Internet in many aspects of their life, revealing extremely sensitive personal information without recognizing the ramifications of data misuse. We believe that as the volume of personal information transmitted over the Internet grows, the challenges surrounding end - user privacy will continue to expand. Furthermore, usability concerns are receiving increased attention as a method to develop end - user oriented security mechanisms that users can intuitively learn and apply to safeguard their data without complexity or a long learning curve.

In the past, the cyber security community has relied on incremental updates to address existing security and privacy vulnerabilities before moving on to the next phase. Since the original Internet was created for a totally different context from how it is used now, some argue that this gradual approach has not worked effectively and will not be able to satisfy future requirements. To make greater use of the Internet's rapidly rising needs, a strategy to think "outside the box" without relying on the present computing system and the Internet but instead beginning something new has been proposed. The Internet's anonymous character has been identified as a cause of escalating cyber attacks, making it harder to track down the perpetrator. Identity management and trace back techniques on a worldwide scale have become a hot topic of research as a strategic strategy to combat a growing number of cyber attackers in the future, particularly where important infrastructure is involved.

In the following sections, we go through each of these potential future study areas in further depth.

**1) Pay special attention to privacy.**

With the increased use of networked systems and the Internet in recent years, privacy has become a crucial concern in the development of IT systems. The Internet is now used in every aspect of our life, necessitating an ever - increasing amount of personal data to be put into cyberspace. This rise in online buying indicates that Internet users are getting more comfortable revealing sensitive financial data like credit card numbers and delivery addresses. Similarly, in the last decade, professional and social networking services that link people with similar interests online have witnessed explosive development. As the amount of information uploaded to the Internet grows, the risks of privacy being compromised grow as well. Individuals' internet visits, for example, are monitored in order to collect information and provide ads depending on their browsing history. Compromise tactics can range from the collection of user statistics to more malevolent acts such as the distribution of malware. Social networking platforms are used by cyber thieves to obtain personal information for use in fraud and identity theft.

Several social networking platforms have privacy protections in place to avoid such data leaks. For example, all Facebook users have access to a privacy setting. The ability to ban particular persons from viewing one's profile, the capacity to designate one's "friends, " and the ability to limit who has access to one's photographs and videos are all options accessible on Facebook. Other social networking services, such as Google Plus and Twitter, include privacy options as well. Children and teenagers are particularly vulnerable to abusing the Internet and, as a result, putting their privacy at danger. Parents whose children are now using Facebook and other social media sites on a regular basis are becoming increasingly concerned.

The purpose of privacy - aware security is to allow people and organizations to better express, preserve, and regulate the confidentiality of their personal data, even when they choose (or are required to) share it with others.

**2) Secure internet of the future**

There's no denying that the Internet has altered and continues to affect how people interact, businesses run, emergency situations are handled, and the military works, among other things. Despite its crucial importance, some parts of the Internet are vulnerable and are continually subjected to attacks ranging from software vulnerabilities to denial - of - service attacks. The Internet architecture and associated protocols were largely intended for a benign and trustworthy environment, with little or no thought for security concerns. This is one of the key causes for these security flaws. Some, on the other hand, argue that Internet technology has reached a stage where users are unable to test new ideas on the present infrastructure. For example, without additional security guarantee, a best - effort IP delivery strategy is no longer regarded appropriate. Routing is no longer centered on algorithmic optimization, but rather on policy compliance in order to support a diverse set of applications. Energy - conscious embedded system networks, such as sensor networks, cannot be integrated with protocols that are not built with energy conservation in mind. Initial estimates of the Internet's size have long been proven incorrect, resulting in the current predicament of IP address shortage. A new architectural design paradigm known as "clean - slate design" has been proposed.

**3) Towards dependable systems**

The majority of today's systems are based on unreliable legacy systems and are constructed with insufficient designs, development techniques, and tools. As a result, they are often unprepared to deal with cyber - attacks. The situation is made worse by the fact that today's devices are themselves networks of systems and components. They must interact with other components and systems in sophisticated ways, which might result in unexpected and potentially harmful behavior. Many systems have claimed to have a trustworthy computing base (TBC) in the past, which was meant to offer a secure basis for the important components. Error - correcting codes, for example, were created to circumvent faulty communication and storage medium. Despite unsafe communication connections, encryption has been employed to enhance secrecy and integrity. Firewalls have also been deployed to safeguard internal assets from external threats. However, because to the ongoing evolution of assaults, the concept of having one precise solution to a given problem has not proven effective.

**4) Identity management and traceback procedures on a global scale**

The task of regulating information about users on computers is known as identity management. Information that authenticates a user's identity, as well as information that defines the information and activities they are authorized to view and/or do, falls under this category. It also involves the administration of descriptive information about the user, as well as how and who may access and modify that information. Users, hardware, network resources, and even programs are examples of managed entities.

When accessing key information technology systems from anywhere, global - scale identity management is concerned with identifying and authenticating things such as people, hardware devices, distributed sensors, and software

applications. Due to the rising usage of mobile phones and embedded sensors in every aspect of our everyday lives, the phrase "global - scale" is intended to stress the ubiquitous nature of identities. This also suggests that in federated systems, identities exist that are outside the control of any particular entity.

**5) Useful safety**

The importance of usable security and the challenges that come with implementing acceptable solutions are becoming increasingly apparent.

Many security methods have attempted to increase usability; nonetheless, the majority of them fall short. Password schemes have long been seen to be one of the most fundamental components of usable security. As a result, a number of complex methods have been developed, such as the frequency with which passwords are changed, the inclusion of non - alphabetic letters, and the use of visual and biometric - based passwords that users do not have to memorize. Despite these efforts, the security risks associated with poorly implemented password systems have been well documented throughout time. Users are forced to scribble them on scraps of paper or save them on unsecured mobile devices.

Mail authentication is another active field in which usable security has been investigated in the form of genuine email sender authentication. Pop - up security dialogs and SSL lock icons have also been proposed. Another issue that makes it difficult to create an effective usable security strategy is that when security is improved, system usability tends to deteriorate. Some email systems, for example, demand users to reauthenticate on a regular basis to ensure that they are the authorized individual.

## 3. Conclusion

This poll focuses on two areas of information systems: recognizing weaknesses in current technologies and potential risks in future telecommunication and information technologies. Emerging technologies, such as social media, cloud computing, smartphone technology, and critical infrastructure, have seen an increase in threats, which frequently take advantage of their particular properties. We discussed the features of each developing technology, as well as the numerous methods through which malware is disseminated in these new technologies. Then we go through a typical set of broad attack patterns that have been discovered in new technologies.

Because most of these developing technologies provide services through the internet, some of the most prevalent assaults are increasingly relying on malware concealed inside extensions or weaknesses in scripting languages to get access to personal data. To evade discovery, adversaries are shifting their battleground from the desktop to other platforms such as mobile phones, tablet PCs, and VoIP. With the expanding number of mobile users and the sophistication of mobile applications, mobile malware has increased dramatically in recent years. Scammers are increasingly employing social engineering techniques. Popular social networking sites such as Facebook, Twitter, and others are increasingly being exploited to trick unwary users into installing or spreading malware. The usage of botnets has been used in more orchestrated attacks. Botnets are a significant source of worry since their impact is far greater than individual attacks. According to recent data, the amount of cyber assaults targeted to a specific system, such as a command and control system, utilizing inside knowledge and employees is on the rise.

We also sketched out some possible future study directions. Understanding all levels of users, including both specialists and non - experts in computer systems, and creating security methods appropriate to their confidence levels has become increasingly important as more people get linked via the Internet.

The future development of next - generation secure Internet and trustworthy systems has been highlighted as significant research areas to consider. The development of global scale identity management and trace back mechanisms to enable tracking down enemies has also garnered traction as a future priority.