WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Cyber Security and Data Privacy: Emerging Threats and Countermeasures - A Survey

Mayuri Hawaldar[#1], Omkar Raikar[#2], Mrutyunjaya Emmi[#3]

MCA Department, Gogte Institute of Technology, Udyambaug, Belgaum, Kanataka, India
[1]2gi21mc044@students.git.edu, [2]2gi21mc059@students.git.edu, [3]msemmi@git.edu

ABSTRACT-

People are highly linked in today's globe thanks to contemporary networks like the Internet. On top of all these components, several applications and services have been created and continue to be built. The ability to share information in the form of files or other data has made it feasible to collaborate on projects at work and has made social interaction simpler. increasing the level of efficiency in the world. However, this has also created several chances for bad actors to exploit connections to carry out harmful actions such as disrupting services, stealing information by gaining unauthorized access or causing harm to people or businesses by exposing sensitive data. Due to this, cyber security and data privacy are now major global concerns.

Keywords— Cyber Security, Countermeasures, Security Threats

INTRODUCTION

Cybersecurity is "the body of technologies, practice with coordinated series of actions, that are designed to defend the Networks, Computers, and System Application Programs and data from an Attack, Damage or Unauthorized Access".

“An attempt to undermine or compromise the function of a computer-based system or attempt to track the online movements of individuals without their permission; Attacks of this type may be undetectable to the end user, or lead to such a total disruption of the network that none of the users can perform even the most rudimentary of tasks” [2].

Cyberattacks are cheaper, easier, and safer than physical assaults. Cybercriminals usually simply need a computer and an Internet connection. They're unbound by distance. Internet anonymity makes them hard to catch and prosecute. Cyber assaults are appealing, thus their quantity and complexity will likely increase. [3]

Cyber security has grown more vital to safeguard persons, firms, and systems from illegal access and exploitation.

I. CYBER SECURITY THREATS

Even for PC clients who are naturally comfortable with the technology and jargon of security specialists, the chore of securing the Web and staying ahead of developing dangers might be a difficult one. Infections with viruses, hacking attempts, or "Phishing scams" are reported every week. Consequently, a variety of PC users, including those who have installed security software like firewalls, anti-virus, and precise filtering software, may be vulnerable to security threats and software malfunctions.

The majority of the time, these threats may be classified as malicious assaults, network attacks, and network abuse.

Keyloggers, Trojan horses, spyware, BOTS, and computer viruses are examples of harmful software. A few examples of network assaults are session hijacking, denial of service (DOS), spoofing, and online defacement. SPAM, phishing, and pharming are examples of network abuses. Some of these risks are essentially discussed below with regard to incidents of network-related forgery:

A. Malicious Attacks

1) Malware and Spyware

Harmful programs that secretly gather computer information, pose significant threats to businesses, governments, and individuals. Many new Malware signatures and variants have surged, driven by illicit financial motives.

Ex: In January 2023, a malware called ‘XLoader’ was discovered. This malware is a Trojan that can steal passwords, banking information, and other sensitive data. It is believed to have been used to target businesses and government agencies in the United States and Europe.

2) Botnet

A botnet is a group of infected systems controlled by a single "Botmaster." These networks, used by cybercriminals for illegal purposes, pose a significant danger to cybersecurity, as they can disrupt and spread harmful code. Figure 1 covers the botnet life cycle.

Ex: In October 2016, a massive botnet called ‘Mirai’ was used to launch a distributed denial-of-service (DDoS) attack on Dyn, a major internet infrastructure company. The attack caused widespread disruptions to websites and online services around the world.

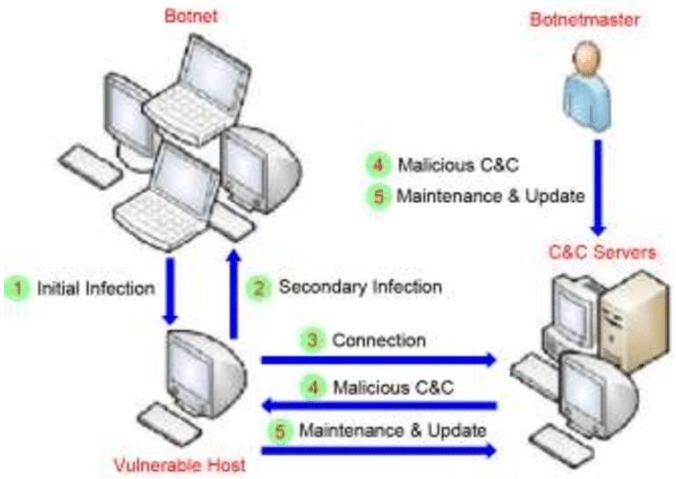

Figure 1: A typical Botnet life Cycle.

3) Key loggers

Keyloggers are programs that secretly record a user's keyboard activity, and capture sensitive data. They can either store the data or covertly send it to other applications. While some keyloggers need the criminal intruder or attacker to have access to the system in order to obtain the data, others forcibly send the data to other machines via email, file transfers, etc. Personal usage of key-loggers may offer benefits such as data recovery after system crashes.

Ex: In June 2022, a key logger called ‘DarkHotel’ was used to target business and government leaders using hotel WIFI. Once that access was gained, the attackers installed key loggers to capture their targets' passwords and other sensitive information.

4) Virus

A virus is software that distributes itself to the corrupted files or programs of a PC without the user's consent and moves from one computer to another. And causes unexpected outcomes. Viruses have various functions, from capturing data to destroying programs. They advertise themselves as email attachments and have the ability to damage computer applications, and can spread through USB and other external storage devices.

Ex: In June 2017, A virus called ‘NotPetya’ was used to attack businesses and government agencies in Ukraine. The virus caused widespread disruptions and damage, and it is believed to have been responsible for billions of dollars in losses.

5) Worm

Worms are self-replicating computer programs that travel from one environment to another, often remembering their former habitat. When entering a new habitat, a worm can do whatever it wants within access limits. Unlike viruses, worms propagate via the internet.

Example: In May 2017, WannaCry attacked companies and governments worldwide. The virus sought a ransom to decrypt a victim's data. It infected over 200,000 machines and cost billions.

B. Network Attacks

1) Denial of Service (DOS)

A DoS attack disrupts the computer system, denying authorized access to expected resources. According to Karthik, these are "incidents in which a Client or organization is denied the services of a resource they would ordinarily expect to have.". It is a resource overloading assault that destroys the host and leaves services unavailable to customers.

Ex: In May 2023, a DDoS attack targeted the website of the BBC. The attack lasted for several hours and disrupted access to the website for millions of users.

C. Network Abuse

1) Phishing and email Spamming

It refers to a form of unwelcome online communication, including but not limited to threats sent through the Internet. These requests use deception tactics to steal the client's credentials.

Law enforcement and the judicial system now seem to start taking cybercrime seriously, A man was apparently "Sentenced to more than twelve years in federal prison" in July 2011 for his part in an international phishing and email spamming network that stole the identities of more than 38,000 people.

2) Social Engineering

Social engineering (SE) is a strategy that involves tricking or trapping consumers or victims into revealing crucial information by gaining their trust.

The users will believe the motivation is sincere, but the end goal is unlawful. Okenyi and Gaudin go on to say that SE depends on people's willingness to be trusted since it relies on impersonating others to obtain confidential information. As a result, SE may be thought of as "the human side of breaking into a corporate network" [2].

Ex: In January 2023, a phishing attack impersonated DoL's (Department of Labor) email addresses to steal personal and financial info from employees. The emails contained malicious links that, when clicked, would install malware on the victim's computer. The attack spread via compromised accounts

II. USER VULNERABILITIES AND THEIR PREVENTION

After installing malware on the victim's system, cybercriminals exploit existing vulnerabilities in hardware, software, and network layers. The current initiatives that have been suggested. along with examples of countermeasures and a list of common attacks in Table 1.

	Hardware	Software	Network
Common Attacks	*Hardware Trojan *Illegal Clones *Side Channel attacks(ie. Snopping hardware signals)	*Software programming bugs(e.g. memory management, race condition. *Software design bugs *Deployment errors	*Network protocol attacks *Network monitoring and sniffing
Examples of countermeasures	*Tamper-Resistant Hardware(e.g. TPM) *Trusted computer base(TCB) *Hardware watermarking *Hardware obfuscation	*Secure coding practice(e.g. type checking, runtime error etc) *Code obfuscation *Formal methods *Secure design &development	*Firewall *Intrusion prevention and Detection *Virtual private network(VPN) *Encryption

Table 1: Common attacks in the Hardware, Software, and Network layers.

A. Hardware

The most powerful component of a computing system and its greatest manipulator is hardware. Its hacking allows attackers a great deal of freedom and power to undertake harmful security assaults at this level.

Unlike software-level assaults, which may be regularly detected by measures like intrusion detection programs, Numerous hardware-based assaults are capable of avoiding such detection.

Hardware Trojan is the most heinous and prevalent kind of hardware abuse. Electronic components, such as Integrated Circuits (IC) in the hardware, are modified maliciously and purposefully by hardware Trojans. These Trojans cause various adverse consequences, such as modifying error detection modules to accept incorrect inputs and altering chip interconnections to increase power consumption. In more severe cases, Denial-of-Service (DoS) Trojans disrupt the function or resource operation.

Side-channel attacks, like examining power use and electromagnetic radiation, can expose sensitive data. The rise of illegally manufactured hardware with harmful backdoors and Trojans increases hardware-based exploitation, including unauthorized hardware clones

To prevent assaults on the hardware level, several methods have been put forth:

1) Tamper-resistant hardware devices

The Trusted Platform Module (TPM) offers secured storage, cryptographic primitives, and the ability to exchange tamper-resistant evidence with distant servers.

2) Trusted Computing Base (TCB)

The Trusted Computing Base (TCB) comprises all essential hardware and software pieces for the system's security. Ensuring no faults or vulnerabilities exist. TCB is crucial to maintaining the system's overall security. Computer-assisted software audit is used to audit the TCB's code base for security assurance.

3) Hardware Watermarking

Hardware Watermarking protects the host item from illicit counterfeiting by encoding ownership information in the circuit's description. Hardware obfuscation, a technique that modifies hardware description or structure, intentionally conceals the hardware's operation to prevent unauthorized access, copying, or counterfeiting.

4) Including Noise

Adding noises prevents physical information from being directly displayed, It filters some physical information and makes/blinds, This aims to eliminate any correlation between the input data and side-channel emission.

B. Software

"Software bug" refers to the flaws in computer programs, Cyberattacks make use of software flaws to make systems act in ways contrary to their intended behavior.

Software defects in memory, user input validation, race situations, and user access rights are the most frequent sources of software vulnerabilities.

Attackers use the following methods :

1) Buffer Overflow

This occurs when software tries to store more data in a buffer than it was designed to contain. This causes excess data to overflow into neighboring buffers and alters the data. It enables attackers to alter the code of active processes. Input validation is used to make sure that the input data complies with specific standards. Data corruption can result from improper data validation.

2) SQL injection

It is one of the most popular methods for exploiting a software flaw on a website. An attacker injects SQL instructions into the web form to alter the database's content or to get sensitive data like credit card numbers and passwords.

3) Race condition error

Adversaries exploit process imperfections that make their output dependent on the timing of other occurrences. The gap between the time a condition is checked and the time its findings are used is known as the time of check to time of usage problem. Also called Race condition error.

4) Privilege confusion

It is when an attacker takes advantage of a flaw to obtain control of a system's restricted resources. As a result, enemies with more access can break in and steal sensitive information, such as keys to a safe.

C. Initiatives

There are now a number of active initiatives whose primary focus is on tightening security. These initiatives aim to build a more safe computer environment:

1) Secure Coding Practice

Software engineers in a code review-based secure coding practice find and fix frequent programming errors that result in software vulnerabilities. And thus create uniform secure coding standards.

2) Addition of Runtime Checks

In this, the program is designed in such a way that it cannot do any changes that would be in violation of certain set policies.

3) Code obfuscation

It's a method for making source or machine code that's incomprehensible to humans. This limits the potential of reverse engineering as codes are obfuscated to hide their functionality or logic.

4) Secure design and development cycle

It provides a collection of design tools that may efficiently verify that a system component has no bugs in its design. Formal techniques are not simple, but they do allow for a thorough investigation of the design and the detection of subtle security flaws.

D. Network infrastructure and protocol vulnerabilities

The original network protocol was designed for a very different, much smaller, environment, and as a result, fails to function correctly in many modern contexts.

Not implementing security filters or policies, using ineffective encryption algorithms, or not updating systems with the latest patches are all examples of administrative errors that can leave systems vulnerable.

Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS) vulnerabilities are frequently targeted in network attacks.

To protect the networks, many solutions have been created:

1) IPSec

IP traffic encryption was a primary motivation for the creation of IPSec. To establish a safe connection between a distant computer and a local, trusted network (such as an organization's intranet), VPNs have increasingly relied on IPSec in recent years. TCP operates on top of IP to provide dependable (by resending missed packets) and sequential transmission of data.

1) SSL

SSL was created as an add-on to the TCP protocol so that data sent between computers are encrypted in transit instead of only at rest. Secure Web sites often employ SSL/TLS in conjunction with HTTP to produce https.

3) Cryptography

It's crucial for ensuring that only the intended recipients may read sent data by encrypting it so that only they possess the decryption keys. When it comes to safeguarding sensitive information, cryptography is the gold standard.[3].

III. COUNTERMEASURES

A. External

Nowadays, a number of charitable organizations, such as Secure Domain Foundation (SDF) and the International Association of Cyber-crime Prevention (IACP), work to prevent cyberattacks by educating Companies and Individuals about the dangers of such attacks, how they can be exposed to them, and how to protect themselves.

Aside from the non-profit organization, Google has also begun building its own team, known as ‘Project Zero’, with the goal of analyzing bugs and vulnerabilities in their own and other companies' software to improve the software products and reduce the risk of cyberattacks.

Financial institutions are now aware of the rising trend of cyber-attacks. Thus, one of the companies, ‘AXA Corporate Solutions’ has introduced an insurance policy to cover costs associated with recovering from a cyber-attack, viruses, mistakes, or unintentional incidents.

Laws and regulations are constantly being developed to prevent or limit cybercrime. However, it is concerning that each set of laws and regulations is geographically limited to a particular state, region, or other location.

B. Internal

1) Continuous risk assessment

No two businesses are alike. Thus every organization has a unique risk profile that is based on factors such as size, location, industry of operation, etc. Each organization should identify its threats, vulnerabilities, and risks and then design and implement measures to address these risks.

2) IT environment’s health

It is important for companies to guarantee that all of their hardware and software, including safety software (such as antivirus programs), is constantly up to date, that the most recent updates are installed, and that there are no exceptions to this rule.

3) Authentication

Access to the programs and data of the organization could only be password-protected, depending on the risk assessment. However, it might be advised to use more complex authentication methods, combining at least two of the following: ‘a password’, ‘a PIN- generating device/key’, and ‘biometric authentication’. Especially for remote access or web-based applications.

4) Internal commitment and responsibility

Given that vulnerabilities are frequently created by security breaches perpetrated (even unintentionally) by the company's own employees, company-wide knowledge is crucial. A set of rules and procedures must be enforced, and presented in a clear and straightforward manner, to enforce employee commitment.

5) Access to information

Businesses should make sure that access to departing employees, contractors, auditors, and other third parties who previously needed connectivity to the company's network is adequately restricted and promptly terminated.

6) Data retention

The quickest and easiest way to ensure the privacy of sensitive data is to get rid of files that are no longer needed for regular business functions. The goal of data archiving and retention is to remove data from the company's network while ensuring its continued availability for as long as required. This lessens the possibility that outsiders may gain access to sensitive data.

7) Other security controls

To protect the confidentiality, integrity, and availability of data, a variety of controls may be put in place depending on the risks that need to be handled. Controls can vary from one business to the next and can be divided into two categories:

a) Preventive controls, which are security measures intended to thwart threats (for example, limiting access to the company's network, programs, and data may stop unauthorized access);

b) Detective controls, which are measures intended to spot threats to information security (for instance, even if unauthorized access was achieved, an intrusion detection system monitors network traffic and spots suspicious activity);

c) Corrective controls - security measures designed to fix discovered abnormalities (such as helping a company recover from an attack) [4].

IV. CYBER-SECURITY OF EMBEDDED IOTS IN SMART HOMES

The Internet of Things (IoT) Devices are Intelligent Objects that are linked to a network to accept commands remotely from a user. They often have sensors to react to their surroundings. Figure 2 depicts an IOT block Diagram.

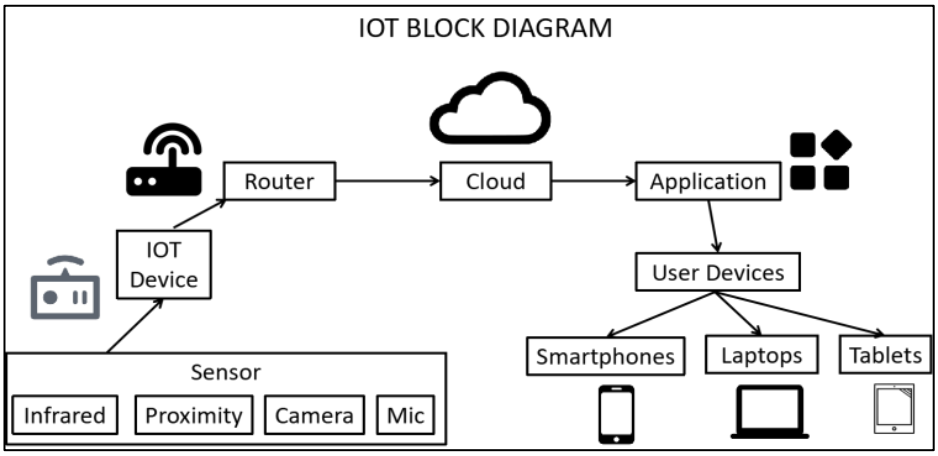

Figure 2: IOT Block Diagram

Users worry that hackers may intrude into the network to obtain private and personal information.

The Internet of Things (IoT) must be open, free, and accessible to everybody, according to Berners-Lee. By 2025, there are projected to be 24 billion gadgets online and in the public domain, which presents a number of security risks that, if not addressed, might result in a number of major issues.

A. Precautions

These are precautions should be followed to prevent such attacks :

1) Checking that the router is configured correctly:

The Wi-Fi routers serve as the gateway in a smart home. These instructions may be used to set up a secure router:

i. Not designating the router with its default name

ii. Make a password that is distinct from the name of the home's occupants

iii. Using data Encryption like WPA3, As supports individual encryption, which prevents devices from accessing each other's data even when they are connected to the same network.

2) Create an IOT-Specific Wi-Fi network:

This helps keep IOT and Private Hotspots separated and makes sure that there is no intrusion into more crucial devices like Laptops.

3) Turn off needless features:

Many Internet of Things (IoT) gadgets may function from any location. Disabling the unnecessary remote access options is strongly advised. Smart speakers, for instance, include Wi-Fi and Bluetooth connection.

A lot of people don't use voice control on smart TVs. Disabling this prevents hackers to listen to your discussions. Thus, Disabling features is all about preventing as many of those numerous access points from being used as feasible.

4) Updating the devices is mandatory:

The Wi-Fi router's firmware may occasionally need to be updated manually. Oftentimes, these releases contain patches for security flaws. Every few months, do a manual check for updates; if any are discovered, it is advised that you download and apply them right away.

5)Activate multi-factor authentication:

Multi-factor authentication, often known as 2FA, is an additional layer of protection that requires more than just a password.

Users are asked to give more identifying information each time they attempt to log into an Internet of Things device. In the event that the Internet of Things device does not, by default, perform two-factor authentication, an alternative authenticator, such as a cloud-based solution, may be employed. [5]

V. CONCLUSION

The global effort to combat cybercrime has a lot of space for growth. Due to a lack of knowledge about these attacks, the globe is having a very difficult time assuring the adequate protection of information.

In our effort to stop individuals from becoming falsely fully imprisoned and exploited, raising knowledge of the hazards and how to recognize them may be very helpful.

Additionally, each nation must have its own set of rules and regulations controlling the infringement of data privacy and theft. Attackers use the internet as a worldwide instrument, thus the only way to stop cybercrime is for authorities to think and act globally, upholding the rights and safety of people all over the world.

Additionally, each person, business, or authority has a duty to maintain a certain standard of security that has been individually assessed and developed in order to support information security and data privacy. This is because each person, business, or authority has the right to control what data is retained, managed, and shared.

REFERENCES

[1] A Literature Review on Threats and Countermeasures of Cybersecurity: A cross-industry analysis in Kathmandu. Neelima Shahi

[2] State of Cyber Security: Emerging Threats Landscape. Alhaji Idi Babate, Maryam Abdullahi Musa, Aliyu Musa Kida, Musa Kalla Saidu, 2018

[3] A survey of emerging threats in cybersecurity. Julian Jang-Jaccard, Surya Nepal,2014

[4] Cyber-Attacks – Trends, Patterns and Security Countermeasures AndreeaBendovschi, 2015

[5] Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends. AaeshaAldahmani, Bassem Ouni (Member, IEEE), Thierry Lestable, And MerouaneDebbah (Fellow, IEEE), 2023