Sri Lanka Institute of Information Technology

IOT ATTACK BY CYBERCRIMINALS

IE2022 – Introduction to Cyber Security

W.N. DILSARA
IT21182600

Contents

Abstract

A revolutionary future where many of our everyday items are networked is being made possible by advanced Internet of Things (IoT) technologies. These things must be able to communicate and interact with one another as well as their environment.This allows many activities to be automated. Interconnecting IoT nodes includes stability, smooth authentication, robustness and simple maintenance. Using Internet of Things technology and various sensing and functional capabilities for smart, intelligent devices that are more realistic but still very attractive targets for cyber-attacks and cybercrimes. has caused Vigilance and preparedness are the main lines of defense against cyber-attacks and cybercrimes. The aim of the research is to identify the attacks on the iot, to avoid such attacks and to analyze the future IoT development and their security. In this analysis, we review the impact of IoT device vulnerability, cyber-attacks and how to survive it and its security posture in the future evolution of IoT based on detailed reports, evaluation criteria and reliable data.

Introduction to the IoT Attack by Cybercriminals

We live in an age where technology is essential for all people. All five aspects of our lives are dependent on technology. Today's world is evolving with the fastest-growing Internet of Things-based applications. The Internet of Things is one of the most enduring technological revolutions of the past two decades. IoT devices are often considered networked computing devices with computing power, sensing capabilities, and the Internet to communicate with each other. IoT growth is considered one of the most popular topics in recent years. IoT is a network-enabled device that excludes traditional computers such as laptops, computers, and servers. Most IoT devices are manufactured to meet the needs of a particular audience of visual users. So, no strict security users use this to attack a communication system through any weak IoT device.

Today, IoT-based computing devices have become the crown jewel of cybercriminals. Out of 42% of businesses worldwide, Ab uses unsecured IoT devices. We must first identify the threats and attacks to make the IoT environment secure and reliable. There are billions of intelligent devices in the world. They are produced and owned by millions of businesses and individuals. Therefore, considering these devices' reliability, security, and privacy criteria is quite a problematic issue. IoT attacks are cyber-attacks that gain access to users' sensitive data through any IoT device. To protect yourself from these attacks, you must first be aware of cyber-attacks. You should also know how to escape from them and not get caught by them. In today's rapidly digitalizing world, people are used to doing everything online. During the last coronavirus pandemic, almost everyone turned to the Internet. Here, many people do not know about cyber security. Today, attackers have started using this advantage.

However, this market regulates the mechanism. Thus data retention and computer preservation cannot be completely ruled out. For instance, a hacker can open a door lock connected to the Internet remotely. Cybercrime will be made possible by data security issues, which will be a huge problem. For the existing level of IoT cybercrime and anticipated future IoT cybercrime,

cybersecurity technologies should be developed. Therefore, this article addresses the key technological developments foreseen in the future.

Evolution of the IoT Attack by Cyber Criminals

Begin IoT

Arpanet, the world's first connected network.The history of IoT began with the inception of Arpanet. 1989 Tim Berners proposed the World Wide Web framework that laid the foundations of the Internet.

In 1990, John Romkey developed a toaster that could be turned on and off over the Internet. [1] This toaster is considered to be the first IoT device. Since then, IoT devices have grown rapidly with the advancement of technology.

Thus, attackers identify their weaknesses when IoT evolution occurs and attack various organizations and individuals. Hacking IoT devices is an advantage for cybercriminals with less effort.

History of the first IoT attack

The world's first malicious program was released into the Internet on November 2, 1988. This cyber worm quickly spread at a remarkable rate and invaded computers. Within 24 hours, approximately 6000 of the 60000 computers connected to the Internet were attacked. [2] The malware did not damage or destroy files, and internet speeds slowed rapidly. The email is days late. Some institutions took down their systems, and others disconnected computers from the Internet. It was complicated to quantify the exact amount of damage done, and estimates started at $100,000 and went up to $1 million. After this incident, cyber-attacks on computers started to be taken more seriously.

What Makes IoT Vulnerable?

Most IoT devices have limited uses and purposes. Because the primary purpose is to achieve simple tasks. A simple IoT device does not have a built-in security solution to prevent typical cyber threats. Some devices have no security features beyond a default password. Because of this,

common vulnerabilities help cybercriminals or groups to use devices in various ways to execute widespread cyberattacks on IoT devices. [3]

In general, unpatched vulnerabilities, lack of adequate security solutions and immutable or insecure passwords can be seen in IoT devices. As the number of ways IoT devices can be connected increases, cybercriminals have more opportunities to exploit. IoT devices are considered the weakest element of a wireless system and are therefore affected by the following factors.

- **Lack of security software:** Most IoT devices do not have the ability to include antivirus or firewall protection. Therefore, it is easily exploited.
- **Lack of cybersecurity awareness:** Many of the fastest-growing industries in the modern world are digitized. But many companies rely on vulnerable IoT devices due to their ignorance.
- **Large attack surface:** Wireless connections between IoT devices represent a broad attack surface with significant access points where hackers can remotely access IoT devices.

Figure 1:Internet Of Things

The Open Web Application Security Project (OWASP), a non-profit foundation for improving software, has published the IoT Top 10 vulnerabilities, [4]

1. **Weak Guessable, or Hardcoded Passwords**

   Weak Guessable and hardcoded passwords are an easy way for attackers to launch large-scale botnets and other malware and compromise IoT devices. Managing passwords in a distributed IoT ecosystem is a time-consuming and difficult task. BecauseIoTt devices are managed wirelessly.

2. **Insecure Network Services**

   Adversaries exploit vulnerabilities in the communication protocol and services running on IoT devices to compromise and compromise sensitive or confidential information exchanged between the device and servers. MITM attacks also target credentials used to leverage credentials to authenticate endpoints and launch broader attacks. to grasp for that too, these weaknesses are exploited.

3. **Insecure Ecosystem Interfaces**

   An authorization mechanism and strong authentication should be in place here. Several solutions have been developed to protect the identity of IoT devices. Whenever a client communicates with an IoT device, the server can distinguish between a valid endpoint and an invalid endpoint by forcing its endpoint to authenticate.

4. **Lack of Secure Update Mechanism**

   Unauthorized software and firmware updates are two major threats to launch attacks IoT devices. Energy and healthcare are particularly vulnerable. Therefore, access to updates must be secured and the source and integrity of updates must be ensured.

5. **Use of Insecure or Outdated Components**

   The security of an IoT ecosystem can be compromised by software dependencies or weaknesses in legacy systems. IoT device manufacturers' use of open-source components to build devices creates a complex supply chain that is difficult to track. These components create a broad threat landscape waiting to be exploited, and attackers can inherit known vulnerabilities.

6. **Insufficient Privacy Protection**

   Many IoT devices collect personal data that needs to be securely stored and processed as they need to comply with various privacy regulations such as gdpr or ccpa. This data may be sensitive or confidential. Lack of appropriate controls may compromise users' privacy.

7. **Insecure Data Transfer and Storage**

   Protecting IoT data at rest or in transit is critical to the reliability and integrity of IoT applications. This data is used in automated decisions or controls that may have serious consequences.

8. **Lack of Device Management**

   A major concern of iot device management is provisioning, operation and updating of devices. One of the most important tasks and one of the most important security challenges is managing all aspects of IoT devices throughout their lifecycle. If unauthorized devices are introduced into the IoT ecosystem, they can monitor corporate networks and gain access and intercept information.

9. **Insecure Default Settings**

   Adversaries can follow hard-coded user passwords, hidden backdoors, and vulnerabilities in device firmware. And having a deep understanding of these settings and the security

gaps they introduce is a first step in implementing appropriate controls to harden these devices.

10. Lack of Physical Hardening

IoT devices are set up in remote and dispersed settings. By obtaining access to the physical layer and making changes, an attacker may interfere with the services provided by IoT devices. For instance, such acts might stop sensors from picking up threats like fire, flood, and sudden movements. We must make sure that the hardware is secure from manipulation, sabotage, physical access, and tampering.

I1	**Weak, Guessable, or Hardcoded Passwords**	Use of easily bruteforced, hardcoded, publicly available, and/or unchangable passwords in client-side software/firmware that can grant unauthorized access to deployed systems.
I2	**Insecure Network Services / Protocols**	Unneeded and/or insecure listening/active network services—especially those exposed to the internet—that compromise confidentiality, integrity, or availability/authenticity of information or allow unauthorized remote remote control, e.g., Telnet, WiFi, ZigBee, Bluetooth, FTP, SSH, UPnP, etc.
I3	**Insecure Access Interfaces**	Insecure web, backend API, cloud, or mobile interfaces that allow compromise of the product and/or its ecosystem. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
I4	**Use of Insecure or Outdated Components**	Use of deprecated and insecure software components/libraries. Insecure customization of operating systems, and use of third-party software or hardware components from compromised supply chain.
I5	**Lack of Secure Update Mechanism**	Lack of ability to securely update the device/ecosystem, lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anit-rollback mechanisms, lack of notifications of security changes due to updates.
I6	**Insufficient Privacy Protection**	User's personal information stored insecurely on device, is used insecurely, improperly, and/or without permission in logs and other artifacts, is transmitted insecurely over the network or the internet, or the system lacks adequate privacy disclosure before usage.
I7	**Insecure Data Transfer and Storage**	Lack of security of sensitive data at rest, in transit, or during processing e.g., weak or lacking cryptography, mismanagement of keys, inefficient platform access controls, insufficient key rotation, absence of secure hardware backed storage.
I8	**Lack of Physical Hardening**	Lack of physical anti-tampering defenses and/or lack of system integrity checking that allows potential attackers to gain sensitive information that can help with a future remote attack.
I9	**Insufficient Security Configurability**	A lack of vendor-provided product features to help the user secure the device through configuration, e.g., stronger authentication, logging and monitoring, encryption strength management, granular policy management, etc.
I10	**Lack of Device Management**	Lack of security support on existing devices deployed in production, including asset management, update management, and secure decommissioning.

Figure 2: OWASP IoT Top 10 vulnerabilities

Common IoT attacks and risks:

➢ Man-in-the-Middle (MITM) Attacks:

Cybercriminals can exploit vulnerabilities in protocol encryption services running on IoT devices using unsecured networks. When they exploit a vulnerability, attackers can breach confidential or sensitive data that must be encrypted between the user and the server. Packets are modified in communication between IoT devices and servers to allow threat actors to obtain malware or to obtain sensitive data from the communication.

➢ Botnet attack IoT:

Botnets are compromised or hijacked computer networks used for activities such as sending spam, distributing malware, and framing DDoS attacks. The permission of the device owner is not mandatory to activate the botnet. The controlling part of the botnet is called the bot header. And each machine on the network is called a bot. The primary purpose of botnet assembly is to facilitate monotonous tasks.

As the number of IoT devices accelerates dramatically, there is a corresponding increase in the number of botnets and cyberattacks. Botnets can be divided into two types.

- **Traditional Botnet;**

  A traditional botnet is a collection of compromised computers or servers. Often referred to as zombies. malware that enables an attacker to take control of them and do actions on their behalf. Through a covert channel like Internet Relay Chat (IRC) or peer-to-peer, botnet owners or herders can manage these infected devices inside the botnet. These controls offer instructions for carrying out actions like distributed denial-of-service (DDoS) assaults, spam, or data theft.

- **IoT Botnets:**

An IoT botnet is a group of hacked IoT devices, such as cameras, routers, and other embedded technologies that have been infected with malware. This software behaves similarly to a conventional botnet. However, compromised IoT devices attempt to spread their virus, unlike conventional botnets. An IoT botnet may have hundreds of thousands of devices as opposed to the thousands that make up a typical botnet.

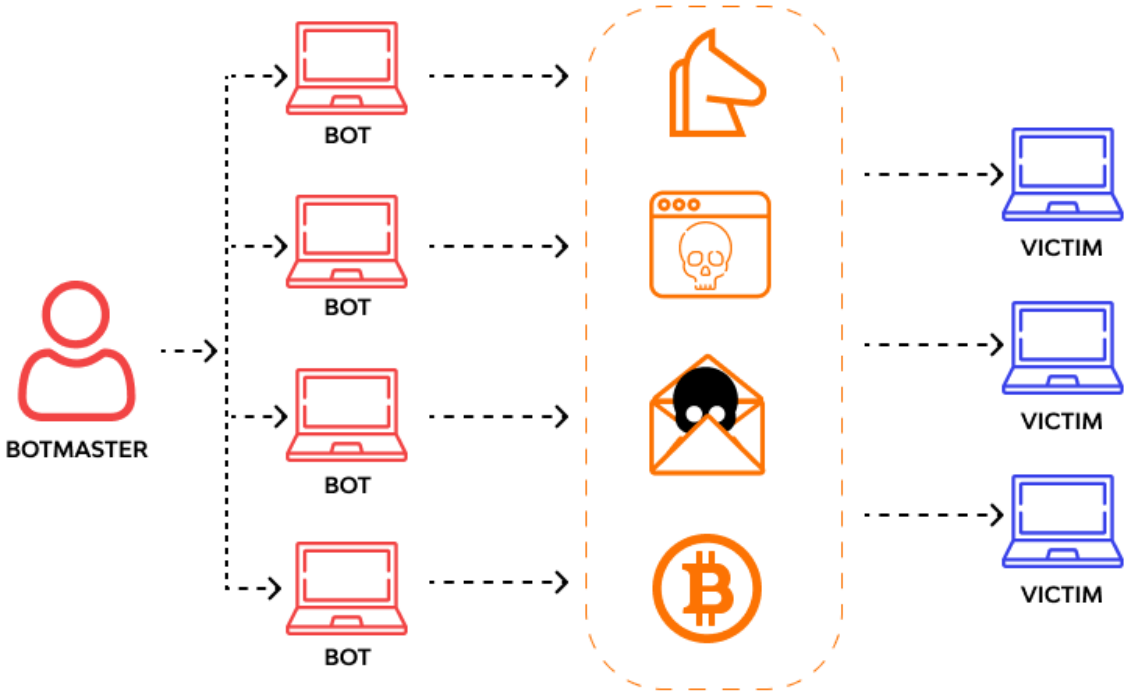

Figure 3: Overview of Botnet Attacks

➢ Types of IoT Botnet Attacks:

There are mainly three types of IoT botnet attacks. Most of these two types of Distributed denial of service (DDoS) and Brute Force Attacks affect IoT devices.

1. **Phishing attack:**

   One of the most common botnet attacks includes criminals or hackers impersonating reliable sources to convince victims to divulge sensitive data, like passwords and bank logins. These details can be used by criminals to steal data and money. Attacks are conducted using various techniques, including email phishing, vishing, and smishing. Phishing attacks targeting large audiences are often carried out by spear and whale fishing

2. **Brute force attacks:**

   Brute force attacks are based on guesswork, accounting for more than 5% of all security breaches. The threat actor keeps trying to guess user credentials until they are successful and they are able to access the target system without authorization. Hit and Trial method works here. It is an easy method that has a higher success rate. Tools for brute force attacks are also available.

   About 84% of organizations in today's world use IoT devices. But about 50% change passwords regularly and follow proper security measures. But some organizations leave the passwords of the IoT devices unchanged or simply set to a default password. Therefore, default, immutable and weak passwords allow cybercriminals to attempt brute force attacks. They use trial and error to crack passwords and access systems, accounts or networks with all possible combinations.

3. **DDoS attacks:**

Distributed denial-of-service attacks are attacks designed to make a computer or cyber service inaccessible by flooding it with traffic from multiple sources. The computer in question typically uses the resources of numerous hosts to create a bottleneck in its traffic flow at busy hours. Stop the administration.

Recently, the number of distributed denial of service or DDoS attacks has increased significantly. That could be due to botnets and Zombified IoT devices. The goal is to attack a single server across multiple devices. Hackers use botnet malware to attempt a DDoS attack via infected or "zombified" IoT devices. [5]

Sample of some large-scale IoT botnet attacks:

- **Mirai Botnet Attack**

  The "Mirai" botnet is the attack method that is credited with popularizing IoT hacking. The Mirai botnet was covered in a study that was released in late August 2016. But as early as 2011, there were attacks on utility systems connected to the Internet. Additionally, security specialists talked about the possibility of hackers gaining access to smart utility meters in houses in 2014. Initial interest in the 2016 Mirai report wasn't very high, but that would all change within a month. With the aid of the Mirai botnet, the first significant IoT attack took place in September 2016. More than 600,000 IoT devices had been infected by Mirai by November 2016. While most of them were Internet routers, several of them were also Internet-connected cameras. [6]

  One of the reasons Mirai spreads so quickly is that it is self-propagating. A replication module scans the entire Internet looking for vulnerable devices. An attack module then performs a Distributed Denial of Service (DDoS)

attack by overwhelming device networks with requests they cannot handle.

- **Zeus Botnet Attack**

  The attack took place in 2007 and is one of the most notorious attacks in history. [7] It was originally designed to obtain the banking information of end users using spam or phishing emails.

  The attack involved the use of a Trojan horse program to infect devices. Since its inception, various variants have been presented. CrytoLockerransomware is an example of this. According to Damballe's estimate in 2009, the botnet infected 3.6 million hosts.

4. **Privilege Escalation Attack**

   Attackers can exploit flaws in an IoT device's operating system to gain unwanted access to a network by identifying critical design flaws, incompatibility vulnerabilities, and operating system flaws. Once they gain unauthorized access, they can use zero-day or unpatched vulnerabilities to gain administrator-level access and control the system.

5. **Malicious Node Injection**

   Information exchange between long-range and power-constrained IoT devices typically passes through multiple nodes, forming a multi-hop mesh network. Multiple security risks, including packet drop attacks, packet attacks, response packet attacks, and others, can affect multi-hop networks. Most of these attacks are executed by malicious nodes and controlled by attackers. [8]

Multiple routing pathways all contain a lot of nodes. A malicious node starts an attack after receiving a message during transmission through it. Attacks against malicious nodes will have a hazy probability in order to elude detection by standard detection techniques.According to some experts, it is possible to ascertain a node's maliciousness or innocence by taking advantage of its trust. It is vital to gather the received messages since the evaluation of the trust levels of the nodes in the Internet of Things is dependent on communication. Sent by each node in the network. Although malicious nodes can be identified, this node-based trust model must add the messages sent by each node and determine each node's reputation value.

However, as the name suggests, attackers use this form of attack to physically place rogue nodes between genuine nodes in an IoT network. The data transmission between the connected nodes can then be managed by these malicious nodes.

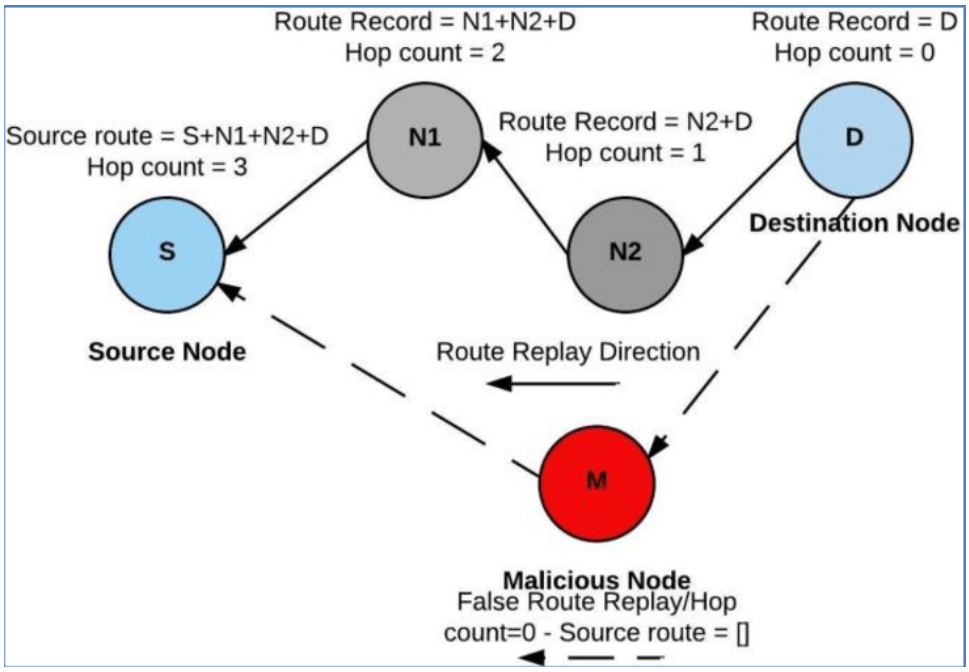

Figure 4: False route Injections

6. **Firmware Hijacking**

   As there are many IoT brands and products, each device has software updates and modifications. Threat actors can take advantage of this unknown environment by uploading fake updates or driver patches to the web. Therefore, drivers of IoT devices should be checked as attackers can hijack the device and download malware.

7. **Eavesdropping**

   Eavesdropping is the act of surreptitiously or surreptitiously listening to the private conversations or communications of others without their consent in order to gather information. [9]

   IoT devices are used by hackers to monitor their victims' networks and steal sensitive data such as login credentials and bank account information. Even when sitting close together, they can hear a conversation going on in a room. This is done by exploiting the unsecured or weakly secured networks that such devices operate on.

8. **Physical tampering**

   In an open environment, IoT devices such as cars are accessible from the outside because there is no control over who can touch them. Hence, attackers establish a foothold through physical tampering to execute a targeted attack.

How does an IoT Attack occur?

- **Early access:**

The attacker first probes with fast scanning tools to find a vulnerable device with an open session. Then the attacker, at that point, gets the IP address of the gadget.

- **Activity:**

After that, a payload or order is executed into the vulnerable device using either exploits or brute force. A shell command is embedded in the operating system (OS) of the device. This forces the operating framework to download a malicious document, at which point it launches a malware payload that performs the dangerous action. [10]

- **Constancy:**

The executed malware payload still resides in some form on the device. It disrupts the monitoring system and creates fresh reports. With the active frame shell of the device exposed, the recursive approach is ready for what's to come.

- **Evasion:**

Utilizing departure techniques enables you to make an effort not to be discovered or identified. The host's security monitoring tools can be removed, the framework logs and order history cleared, the payload document disguised with a parody filename, and hostile troubleshooting and anti-VM techniques used, to mention a few examples.

- **Getting of information:**

All information about the device is added private keys and Bitcoin wallets are stored here, among other sensitive data

- **Regulation & Authority:**

Depending on the orders from the C&C server, the malware payload performs insecure activities, for example, TCP flooding, UDP flooding, and other equipment corruption. HTTP, IRC, P2P, and various other conventions are used for C&C channels. [10]

- **Horizontal Movement:**

After gaining access to the organization's main device, the attacker uses horizontal development techniques to access the other weak devices, which he then targets one at a time. For example, an edge switch is quickly infected and then, at that point, spreads to all other related IoT gadgets.

- **Impact:**

The most likely outcomes of malicious actions on an IoT device include information encryption for recovery, full circle and information collapse, and misuse of coin mining. A malicious virus can "block" an IoT device by completely resetting its partition boundaries or erasing its capacity limit.

How to Prevent IoT Attacks?

Cybercriminals often take advantage of the weakest link in a network's security. Employees don't know how to spot a phishing attack. Poorly secured devices can pose serious risks. And using the device manufacturer's default password is a serious risk.

1. Change the default settings and passwords

When setting up a new IoT device, steps should be taken to disable unnecessary access and connectivity features because there are various connectivity features that can be

useful in some cases but can be dangerous in others. Devices often ship with minimal security features and weak default passwords.

Default Remote Access

Also equipped with features like remote access that some IoT devices don't need. But it is advisable to disable such features if not required.

Most IoT devices come with password protection options. Thus preventing users from using the device without changing the default security settings. Because cybercriminals often use manufacturer resources to guess or search for these default passwords. [11] Using a strong password instead of a default password can protect IoT devices from hackers.

2. Use Multi-Factor Authentication

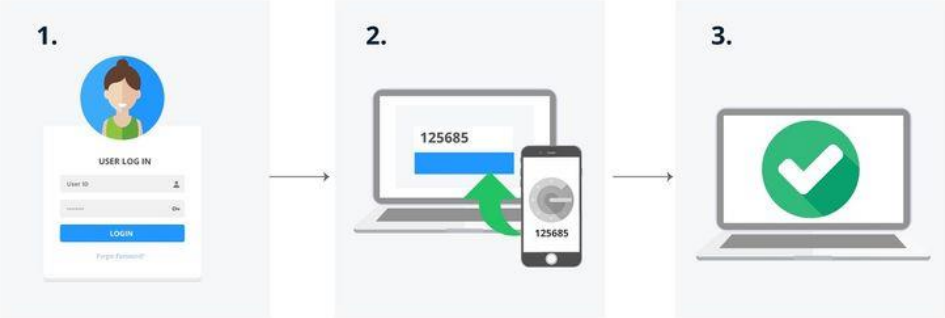

Figure 5: Multi-Factor Authentication

MFA, or multi-factor authentication, is the most popular login technology on the market right now. It is practical and safe as it is simple to use but incredibly safe. MFA works by using an identity verification to validate login attempts. For example, you may need to verify your identity during an MFA login by entering a secure one-time code assigned to a Verified phone number or email address. These codes are unpredictable, almost impossible to guess, and are only valid for a predetermined time. [12]

MFA is extremely secure, even if your password is stolen, a hacker would have to jump through many hoops to access your account. You'll need to steal the password for the account, website, or app you're trying to log in to, as well as your physical phone or email password. The majority of hackers will not bother to attempt this level of difficulty.

Furthermore, most of the major email service providers are quite challenging to hack, let alone access someone's text messages.

Not all devices, IoT hubs, or IoT applications support MFA. But if it is, go ahead and choose to use it. MFA significantly improves IoT security and adds only a minute to your login time. [12]

3.Keep Software Updated

Most cybersecurity applications use databases of malware and virus signatures, or files that allow the software to identify specific viruses. Today, however, security risks are always changing and evolving. To ensure that you are not exposed to fresh dangers, you should keep your security software up to date. Check back often for updates. Security applications regularly release updates that include patches for new threats.

The operating system for your gadgets follows the same principle. While security software may receive updates more regularly than operating systems, it is still crucial to check for upgrades. Older operating systems typically have weakened or outdated security measures, which hackers can take advantage of.

4. Use Strong Wi-Fi Encryption

The operating system for your gadget follows the same principle. Although security software may receive more regular updates than operating systems, it is still very important to check for upgrades. Older operating systems usually have weak or outdated security measures; which hackers can take advantage of.

5.Monitoring Network Activity

You can keep a constant eye on network activity. Using network traffic analysis tools and cybersecurity platforms you can identify odd network events that may point to an attack or network breach. Tracking network traffic for smart homes is now possible thanks to increasingly consumer-centric network traffic monitoring technologies. These tools monitor network activity for you and provide you with alerts when there is unexpected traffic or a malicious network problem.

You can monitor network performance using these tools. Using one of these tools, you may be able to determine why your Internet connection is running slower than you expected. For example, unattended streaming services and background downloads can use up the bandwidth of your Internet connection and slow it down. These offers will be displayed.

Figure 6: Analyze Network Usage in Linux

Future security development and challenges of IoT

A network of physical items that are linked to the Internet and can be accessed, shared, and viewed there is known as the Internet of Things (IoT). Data collection and sharing via various protocols is made possible by the installation of these artefacts in electronics (transceivers and microcontrollers), sensors, software, actuators, and network connections. The standard of living is evolving gradually and will undergo considerable change in the next years. In 2003, there were only 500 million computers connected to the Internet; as of 2022, there are more than 38.6 billion machines connected to the Internet. According to Cisco, 20 trillion devices will be configured with a unique identifier by the year 2030, compared to 500 billion devices in 2030 and 2050.This can be seen in that they can be extremely useful in the fields of electricity, safety and protection, engineering, industry, retail, education, the welfare of the elderly and people with disabilities, the environment, entertainment, travel, smart cities, and much more.

The Internet has evolved from a novelty to a necessity during the past 30 years. Predicting whether we can stay safe in a hyper-connected environment for the next 30 years is a difficult task. Still, analysts anticipate that "deep fakes" and smart cities will be two of the major information security dangers in the future. Intelligent meters and lighting apps, together with voice assistants, are already becoming commonplace. By incorporating the "IoT" into modern technology and the built environment, smart cities would advance.Adding IoT devices is simply one aspect of convenience; another is enhancing control over several automated procedures. According to market research firm IoT Analytics, there will be 13 billion linked IoT endpoints worldwide in 2022. The future will see an increase in this number. Virtual helpers like Siri and Alexa have made it easier for people to interact with networks of linked devices. The future of connecting smart cities may not be a pipe dream if the IoT sector keeps progressing. The security of IoT devices, however, continues to be an unsolvable problem.

Predictions for IoT security

IoT devices are susceptible to malware and cyberattacks because they are always linked to the internet. Future security enhancements will be more and more crucial. Additionally, customers are willing to pay more for enhanced security measures.

1. **Automotive IoT will advance**

   While businesses have made significant investments in consumer IoT products for the smart home, automotive IoT is the wave of the future. The emergence of autonomous vehicles has given the automotive IoT sector some promising new opportunities. As customers entrust their lives to their cars, security concerns associated to automotive IoT will continue to be a crucial component of the sector. Any cyberattack or malicious software can claim life..

2. **IoT technology will still see slow adoption**

   Although market participants have made investments in the technology, consumers are still hesitant to adapt to the evolving IoT market. Despite the fact that the use of IoT devices has significantly risen, the general public is still generally unprepared to adopt voice-enabled gadgets in the linked world. Companies must have patience when dealing with slow-moving markets and negative investment outcomes.

3. **5G infrastructure will grow**

   The introduction of 5G infrastructure is anticipated to grow the IoT sector. But there are a few difficulties that 5G technology might bring to the IoT sector. The development of IoT-connected devices depends heavily on the capabilities of 5G networks.And the specific security issues of 5G networks have yet to be addressed. As IoT devices proliferate with connectivity, so does more attack surface. [13]

4. **Consumer IoT will implement hardware firewalls**

IoT devices, faster and more affordable than traditional alternatives, have been developed by startups and major market players. As consumers are more concerned about the privacy and security of IoT devices, security needs to be improved. For the security of these devices, IoT hardware firewalls will be used to ensure protection from hacking, viruses and phishing scams.

5. **Cybersecurity for smart homes will increase**

Smart homes have become incredibly popular in the last few years. A home IoT network requires a high level of IoT security measures, opening up new potential for diversification in the security market. More businesses will provide security services for smart home networks. Currently, security services are used by a specialist who creates IoT devices and provides IoT services. [14]

Conclusion

This article discusses the changes that have taken place in IoT from the history of IoT till today and what may happen in the future. But mainly, we have reported cyber-attacks on IoT devices. Examples of past cyber-attacks and their negative consequences are shown. Key risks and drawbacks of upcoming IoT devices, along with technological advancements, are also summarized. Some other key concerns are the rapidly evolving nature of technology and the technology life cycle, which contribute to the security challenges that must be addressed. Security will remain a buzzword for the next 30-40 years, but it is truly called the engine of the industry. With so many technical issues and improvements, cybersecurity should be a key part of the technology establishment, but the struggle over privacy and security and law enforcement will continue.

Finally,

Your IoT networks, systems, and infrastructure are compromised by IoT cyberattacks. Cybercriminals may also target your IoT software and devices. You must use tools like internet security and a strong password to secure your gadgets. Make your IoT users aware of cybersecurity best practices as well, such as avoiding phishing emails. Work with a trustworthy IoT vendor as well. For best protection, make sure security is incorporated into product design. Threats won't need to be as concerning, and you may concentrate more on getting things done.

References

[1] A. A. J. J. R. K. M. A. M. A. N. M. Y. A. Abdullah Al, "A Noble Proposal for Internet of Garbage Bins (IoGB)," [Online]. Available: https://www.researchgate.net/publication/356876316_A_Noble_Proposal_for_Internet_of_Garbage_Bins_IoGB.

[2] "The Morris Worm," 2 November 2018. [Online]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

[3] S. J. W.-H. L. C. L. H. W. J. W. P. Z. L. F. Binbin Zhao, "A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices," IEEE, 2022.

[4] "OWASP Internet of Things Project," [Online]. Available: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10.

[5] B. J. K. K. Dhruba Kumar, DDoS attacks: evolution, detection, prevention, reaction, and tolerance, New Yoark : CRC Press, Taylor & Francis Group, 2016.

[6] "The Evolution of IoT Hacking," [Online]. Available: https://www.iotforall.com/evolution-iot-hacking.

[7] "The Life and Death of the Zeus Trojan," [Online]. Available: https://www.malwarebytes.com/blog/news/2021/07/the-life-and-death-of-the-zeus-trojan.

[8] A. K. H. A. K. K. H. Y. Yeliz Yengi, "Malicious Relay Node Detection with Unsupervised Learning in Amplify-Forward Cooperative Networks," IEEE, Sakhier, Bahrain, 2019.

[9] "Wiki Pedia," [Online]. Available: https://en.wikipedia.org/wiki/Eavesdropping.

[10] "8 Stages of the IoT Attack Lifecycle," [Online]. Available: https://www.paloaltonetworks.com/resources/8-stages-of-the-iot-attack-lifecycle.

[11] A. Gupta, The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things, Apress, 2019.

[12] A. I. A. Bandar Omar ALSaleem, "Multi-Factor Authentication to Systems Login," IEEE, Taif, Saudi Arabia, 2021.

[13] X. C. H. A. S. Trung Q. Duong, Ultra-Dense Networks for 5G and Beyond: Modelling, Analysis, and Applications, WILEY, 2019.

[14] "Smart Home Security: Security and Vulnerabilities," [Online]. Available: https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities.