UNIT-1

IOT SECURITY

WHAT IS IOT?

- The Internet of Things (IoT).
- It describes the network of physical objects—“things”—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

IOT SECURITY:

Internet of Things (IoT) devices are computerized Internet-connected objects, such as networked security cameras, smart refrigerators, and WiFi-capable automobiles. IoT security is the process of securing these devices and ensuring they do not introduce threats into a network.

- IoT security is the technology segment focused on safeguarding connected devices and networks in the internet of things (IoT).
- IoT involves adding internet connectivity to a system of interrelated computing devices, mechanical and digital machines, objects, animals and/or people.
- Each "thing" is provided a unique identifier and the ability to automatically transfer data over a network.
- Allowing devices to connect to the internet opens them up to a number of serious vulnerabilities if they are not properly protected.

Anything connected to the Internet is likely to face attack at some point. Attackers can try to remotely compromise IoT devices using a variety of methods, from credential theft to vulnerability exploits. Once they control an IoT device, they can use it to steal data, conduct distributed denial-of-service (DDoS) attacks, or attempt to compromise the rest of the connected network.

IoT security can be particularly challenging because many IoT devices are not built with strong security in place — typically, the manufacturer's focus is on features and usability, rather than security, so that the devices can get to market quickly.IoT devices are increasingly part of everyday life, and both consumers and businesses may face IoT security challenges.

Overview of Security:

Security is **concerned with ensuring legitimate use, maintaining confidentiality, data integrity, and auditing in the network**. Security Management involves identifying the assets, threats, vulnerabilities, and taking protective measures, which if not done may lead to unintended use of computing systems.

Network Security protects your network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.

Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security (endpoint, web, wireless), firewalls, VPN encryption and more.

Privacy in Information system:

Data privacy, also called information privacy, is **an aspect of data protection that addresses the proper storage, access, retention, immutability and security of sensitive data**.

It is a strategic goal that seeks to guarantee the confidentiality of confidential and personally identifiable information (PII) stored on computer systems.

An important goal of data privacy is to ensure that data in transit and data at rest is always protected while still allowing the flow of information.

Principals of IOT Security:

- **No Universal Passwords**
- **Secured Interfaces**
- **Proven Cryptography**
- **Security by Default**
- **Signed Software Updates**
- **Software Updates Applied Automatically**
- **Vulnerability Reporting Scheme**
- **Security Expiration Date**

Principle 1–No Universal Passwords

Often, high-volume consumer devices are all shipped with the same default password. Typically, users want to quickly deploy their new device, so many do not take the simple step of changing the default password to a new one. Shipping each new device with a unique factory-programmed password is a simple first step in making it more difficult for adversaries to gain access to or take control of, potentially, hundreds of deployed devices.

Principle 2–Secured Interfaces

Any microcontroller-based device has a multitude of interfaces and ports that can be accessed either locally or remotely. The primary application will use some of these ports during operation and for communications. However, the rest–particularly any that function as external communication interfaces must be secured. Likewise, any IC-to-IC interfaces—such as between the microcontroller and a display controller—must be secured. It is recommended that all interfaces be encrypted and authenticated during use.

Principle 3–Proven Cryptography

In a world of open and interoperable technologies, the use of industry-recognized, open, and proven cryptographic standards is essential. The use of closed, proprietary cryptographic algorithms is not recommended. The use of open cryptographic standards encourages participation by all developers, engineers, and stakeholders to be continually evaluated for potential vulnerabilities against new security threats.

Principle 4–Security by Default

It is essential that when a consumer purchases a new device, it is already set for the highest possible levels of security. Shipping a product with no or minimal security options configured can pave the way for adversaries to take advantage. The consumer out-of-box security experience should be that all possible security measures are enabled. Developers should not leave a consumer unprotected by default.

Principle 5–Signed Software Updates

With the increasing number of consumer smart-home devices that can update themselves automatically over the air being shipped, the priority is that every update should be signed cryptographically. In this way, hackers are prevented from attempting to update a device with malicious code.

Principle 6–Software Updates Applied Automatically

Consumers shouldn't have to become administrators of their own devices, faced with deciding whether to update a product's software image. If an update needs to be made, it should be deployed and implemented automatically. Moreover, updates should be applied at times when they will not compromise the device's operation. For example, a smart-connected washing machine should not be updated while the machine is in use.

Principle 7–Vulnerability Reporting Scheme

Often, consumers who experience a problem with their embedded smart-home device are unsure who to contact. Has it been compromised? Is there a new vulnerability that should be reported? This principle pledges that product manufacturers will create a means for customers to report problems and communicate their concerns regarding product security.

Principle 8–Security Expiration Date

As with product warranties, which have an expiration date after purchase, the period during which security updates are available should also be defined and communicated to the consumer. Continuing to support a product with security updates involves continued engineering costs, so consumers need to make informed decisions at the time of purchase. Manufacturers also have the option to offer extended warranties to offset ongoing security updates.

IOT Security Guidance:

- Device and data security, including authentication of devices and confidentiality and integrity of data
- Implementing and running security operations at IoT scale
- Meeting compliance requirements and requests
- Meeting performance requirements as per the use case

Key Functional Blocks

IoT security solutions need to implement the functional blocks listed below as interconnected modules, not in isolation, to meet the IoT scale, data security, device trust and compliance requirements.

- **Device Trust:** Establishing and managing Device Identity and Integrity
- **Data Trust:** Policy driven end-to-end data security, privacy from creation to consumption

- **Operationalizing the Trust:** Automating and interfacing to the standards based, proven technologies/products.

Identify the known threats, risks, vulnerabilities and privacy issues:

Threats:

- A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization.
- There are different kinds of network threats, and each has different goals. Some, like distributed denial-of-service (DDoS) attacks, seek to shut down your network or servers by overwhelming it with requests. Other threats, like malware or credential theft, are aimed at stealing your data. Still others, like spyware, will insert themselves into your organization's network, where they'll lie in wait, collecting information about your organization.

There are four main kinds of network threats:

- **External threats:** Threats made by outside organizations or individuals, attempting to get into your network.
- **Internal threats:** These are threats from malicious insiders, such as disgruntled or improperly vetted employees who are working for someone else. These are common. According to Forrester, 46% of breaches in 2019 involved insiders like employees and third-party partners.
- **Structured threats:** Organized attacks by attackers who know what they're doing and have a clear aim or goal in mind. State-sponsored attacks, for example, fall into this category.
- **Unstructured attacks:** Disorganized attacks, often by amateurs with no concrete goal in mind.

1. Malware

Short for "malicious software," malware comes in several forms and can cause serious damage to a computer or corporate network. There are various forms of malware ranging from viruses and worms to Trojans and beyond. Malware is often seen as a catch-all term that refers to any software designed to cause damage to a computer, server, or network.

Antivirus software is the most known product to protect your personal devices against malware and is a great start to prevent potential threats. While for enterprises, protecting your endpoint is essential to quickly detect, prevent, and correct advanced threats to your business.

2. Virus

They have the ability to replicate themselves by hooking them to the program on the host computer like songs, videos etc and then they travel all over the Internet. The Creeper Virus was first detected on ARPANET. Examples include File Virus, Macro Virus, Boot Sector Virus, Stealth Virus etc.

3. Worms

Worms are also self-replicating in nature but they don't hook themselves to the program on host computer. Biggest difference between virus and worms is that worms are network-aware. They can easily travel from one computer to another if network is available and on the target machine they will not do much harm, they will, for example, consume hard disk space thus slowing down the computer.

4. Trojan

The Concept of Trojan is completely different from the viruses and worms. The name Trojan is derived from the 'Trojan Horse' tale in Greek mythology, which explains how the Greeks were able to enter the fortified city of Troy by hiding their soldiers in a big wooden horse given to the Trojans as a gift. The Trojans were very fond of horses and trusted the gift blindly. In the night, the soldiers emerged and attacked the city from the inside.

5. Bots

can be seen as advanced form of worms. They are automated processes that are designed to interact over the internet without the need for human interaction. They can be good or bad. Malicious bot can infect one host and after infecting will create connection to the central server which will provide commands to all infected hosts attached to that network called Botnet.

Risks:

Internet-enabled devices pose a number of security challenges. But while the Internet of Things has brought connectivity to new devices, the general cybersecurity issues aren't really new. We've been dealing with hackers for as long as we've enjoyed the benefits of the Internet.

1. Weak authentication

Passwords are one of the first lines of defense against hacking attempts. But if your password isn't strong enough, your device isn't secure enough. Most default passwords aren't relatively weak—because they're intended to be changed—and in some cases they may be publicly accessible or stored in the application's source code. (That's extremely risky.)

End users may also set the password to something that's easy to remember. But if it's easy to remember, it's probably easy to penetrate.

Many IoT devices have little or no authentication at all. Even if there's no important data stored on the device itself, a vulnerable IoT device can be a gateway to an entire network, or it can be assimilated into a botnet, where hackers can use its processing power to distribute malware and distributed denial of service (DDoS) attacks

Weak authentication is a serious IoT security concern. Manufacturers can help make authentication more secure by requiring multiple steps, using strong default passwords, and setting parameters that lead to secure user-generated passwords.

2. Low processing power

Most IoT applications use very little data. This reduces costs and extends battery life, but it can make them difficult to update Over-the-Air (OTA), and prevents the device from using cybersecurity features like firewalls, virus scanners, and end-to-end encryption. This ultimately leaves them more vulnerable to hacking.

3. Legacy assets

If an application wasn't originally designed for cloud connectivity, it's probably ill-equipped to combat modern cyber attacks. For example, these older assets may not be compatible with newer encryption standards. It's risky to make outdated applications Internet-enabled without making significant changes—

but that's not always possible with legacy assets. They've been cobbled together over years (possibly even decades), which turns even small security improvements into a monumental undertaking.

4. Shared network access

It's easier for IoT device to use the same network as the end user's other devices—such as their WiFi or LAN—but it also makes the entire network more vulnerable. Someone can hack an IoT device to get their foot in the door and gain access to more sensitive data stored on the network or other connected devices. Likewise, another device on the network could be used to hack the IoT device. In either of those scenarios, customers and manufacturers wind up pointing fingers at each other.

Every IoT application should use a separate network and/or have a security gateway or firewall—so if there's a security breach on the device, it remains isolated to the device. (This is one of the advantages of cellular IoT.) A Virtual Private Network (VPN) helps protect your devices from outside the network, but if your application shares a connection with other devices, it's still vulnerable to attacks from them if they become corrupted.

5. Inconsistent security standards

Within IoT, there's a bit of a free-for-all when it comes to security standards. There's no universal, industry-wide standard, which means companies and niches all have to develop their own protocols and guidelines. The lack of standardization makes it harder to secure IoT devices, and it also makes it harder to enable machine-to-machine (M2M) communication without increasing risk.

6. Lack of encryption

One of the greatest threats to IoT security is the lack of encryption on regular transmissions. Many IoT devices don't encrypt the data they send, which means if someone penetrates the network, they can intercept credentials and other important information transmitted to and from the device.

7. Missing firmware updates

Another of the biggest IoT security risks is if devices go out in the field with a bug that creates vulnerabilities. Whether they come from your own developed code or a third party, manufacturers need the ability to issue firmware updates to eliminate these security risks. Ideally, this should happen remotely, but that's not always feasible. If a network's data transfer rates are too low or it has limited messaging capabilities, you may have to physically access the device to issue the update.

Vulnerabilities:

When your computer is connected to an unsecured network, your software security could be compromised without certain protocols in place. Forgetting updates, product weakness and unresolved developer issues leave your clients wide open to computer security vulnerabilities. Here is a list of several types of vulnerabilities that compromise the integrity, availability, and confidentiality of your clients' products.

The most common software security vulnerabilities include:

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs in a security decision
- Cross-site scripting and forgery
- Download of codes without integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Bugs
- Weak passwords
- Software that is already infected with virus

Privacy Issues:

The Difference between Security and Privacy?

Security is about the safeguarding of data, whereas privacy is about the safeguarding of user identity. The specific differences, however, are more complex, and there can certainly be areas of overlap between the two.

- **Security** refers to protection against the unauthorized access of data. We put security controls in place to limit who can access the information.
- **Privacy** is harder to define, in part because user-specific details can also be secure data. In the coming month, we will have a blog with more information on Personally Identifiable Information (PII).

For example, hospital and clinic staff use secure systems to communicate with patients about their health, instead of sending information via personal email accounts. This type of data transmission is an example of security. On the other hand, privacy provisions, might limit patient health record access to specific hospital staff members, such as doctors, nurses, and medical assistants. Privacy might also stipulate *when* users can access specific information (i.e. business hours only).

The major issues concerning online privacy.

1. Spying and Snooping

When you are online, you are spied by a number of trackers for various purposes. Trackers keep a record of your search history and track all your online activities through various means. This provides them a clear picture of who you are and your interests, which is a breach of online privacy policy and makes you a public property. Most of the time, this tracking is for advertisement purposes only and it allows advertisers to show ads according to your taste and interests. But sometimes this information is used by cybercriminals to carry out unauthorized and illegal activities risking your online existence.

2. Information Mishandling

There are various sites on the internet that need your personal information to get access to their services. These sites often store cookies and save your personal information and later use it for various purposes. Most of the time this information is not encrypted and can be accessed by anyone. This mishandling of personal information may lead to serious consequences. The modern trend of e-banking and e-business portals have multiplied the risks associated with online privacy. By sharing your bank details and crucial files on the internet, you are paving ways for burglars and making yourself vulnerable to cybercriminals.

3. Location Tracking

Most of the internet users proudly upload their social media posts highlighting their current location along with tagging friends and family members. It's fun and exciting to share your life events with friends and family, but this data does not remain restricted to your expected audience only. This same data is stored on the social media site you are using and stays there forever, often without you knowing (though you may have given consent through a terms and services agreement). Along with social media apps, Google Maps and other apps also ask for your location and by turning on your location you are providing first-hand information to the world about where exactly you are and what your next move is, which is certainly risky and insecure.

Security Architectures:

- Security architecture is a means to reduce the risk of cyber breaches and protect your assets from digital harm.

The key attributes of security architecture are as follows:

Relationships and Dependencies: Signifies the relationship between the various components inside IT architecture and the way in which they depend on each other.

Benefits: The main advantage of security architecture is its standardization, which makes it affordable. Security architecture is cost-effective due to the re-use of controls described in the architecture.

Form: Security architecture is associated with IT architecture; however, it may take a variety of forms. It generally includes a catalog of conventional controls in addition to relationship diagrams, principles, and so on.

Drivers: Security controls are determined based on four factors:

Risk management

Benchmarking and good practice

Financial

Legal and regulatory

The key phases in the security architecture process are as follows:

Architecture Risk Assessment: Evaluates the business influence of vital business assets, and the odds and effects of vulnerabilities and security threats.

Security Architecture and Design: The design and architecture of security services, which facilitate business risk exposure objectives.

Implementation: Security services and processes are implemented, operated and controlled. Assurance services are designed to ensure that the security policy and standards, security architecture decisions, and risk management are mirrored in the real runtime implementation.

Operations and Monitoring: Day-to-day processes, such as threat and vulnerability management and threat management. Here, measures are taken to supervise and handle the operational state in addition to the depth and breadth of the systems security.