III. IOT SECURITY

III.1. IoT security, risks and vulnerabilities

IoT security and privacy issues

The internet of things connects billions of devices to the internet and involves the use of billions of data points, all of which need to be secured. Due to its expanded attack surface, IoT security and IoT privacy are cited as major concerns.

Machines and objects in virtually any and every industry can be connected and configured to send data over cellular networks to cloud applications and backends.

The digital security risk is present at every step along the IoT journey, and there is a bunch of hackers that would take advantage of a system's vulnerability.

Unfortunately, diverse data type and computing power among IoT devices means there's no 'one size fits all' cybersecurity solution that can protect any IoT deployment.

The first step for any IoT business is to undergo a thorough security risk assessment that examines vulnerabilities in devices and network systems as well as in user and customer backend systems.

Risk must be mitigated for the entire lifecycle of the deployment, especially as it scales and expands geographically.[1]

In 2016, one of the most notorious recent IoT attacks was Mirai, a botnet that infiltrated domain name server provider Dyn and took down many websites for an extended period of time in one of the biggest distributed denial-of-service (DDoS) attacks ever seen. Attackers gained access to the network by exploiting poorly secured IoT devices.

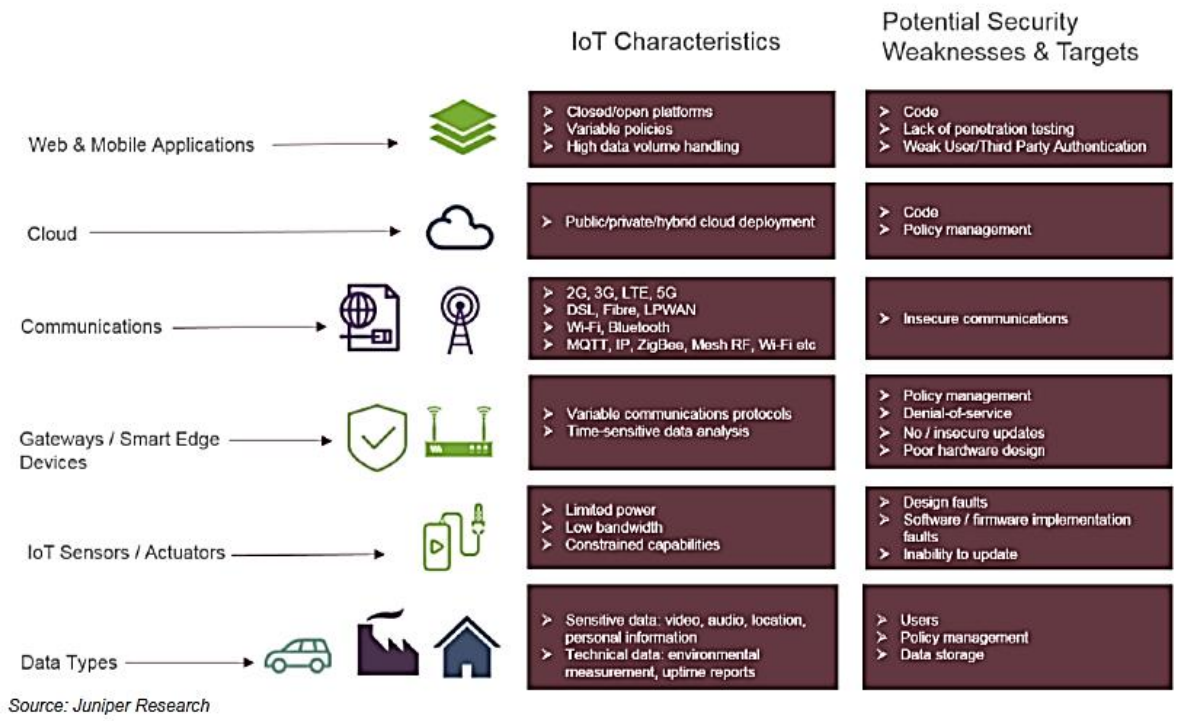
Because IoT devices are closely connected, all a hacker has to do is exploit one vulnerability to manipulate all the data, rendering it unusable. Manufacturers that don't update their devices regularly -- or at all -- leave them vulnerable to cybercriminals.

Additionally, connected devices often ask users to input their personal information, including names, ages, addresses, phone numbers and even social media accounts -- information that's invaluable to hackers.

Hackers aren't the only threat to the internet of things; privacy is another major concern for IoT users. For instance, companies that make and distribute consumer IoT devices could use those devices to obtain and sell users' personal data.

Beyond leaking personal data, IoT poses a risk to critical infrastructure, including electricity, transportation and financial services.

[1] https://www.gemalto.com/iot/iot-security



Source: https://www.gemalto.com/iot/iot-security

Factors impacting IoT security

Data based decisions need reliable data. Vital decisions related to business, safety and health are increasingly based on data. To make the right decisions, data must be accurate and secure.

Different devices require different solutions. Devices come in different in shapes and forms. Some devices are capability constrained with very limited capabilities and for such devices traditional security methods are not possible to use.

End-to-end ecosystems security. In IoT, success depends on collaborative ecosystems of device manufacturers network providers, platform providers, app developers and end-users. Ensuring end-to-end security of the ecosystem is crucial.

Threats

[2]A threat is an action that takes advantage of security weaknesses in a system and has a negative impact on it. Threats can originate from two primary sources: humans and nature. Natural threats, such as earthquakes, hurricanes, floods, and fire could cause severe damage to computer systems. Few safeguards can be implemented against natural disasters, and nobody can prevent them from happening. Disaster recovery plans like backup and contingency plans are the best approaches to secure systems against natural threats. Human threats are those caused by people, such as malicious threats consisting of internal (someone has authorized access) or external threats (individuals or organizations working outside the network) looking to harm and disrupt a system. Human threats are categorized into the following:

[2] https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4

Unstructured threats consisting of mostly inexperienced individuals who use easily available hacking tools.

Structured threats as people know system vulnerabilities and can understand, develop and exploit codes and scripts. An example of a structured threat is Advanced Persistent Threats (APT). APT is a sophisticated network attack targeted at high-value information in business and government organizations, such as manufacturing, financial industries and national defense, to steal data.

Vulnerabilities in IoT Systems

Let us discuss some of the vulnerabilities that IoT sytems are facing:

1. Absence of Transport layer security: In most of the IoT systems data is stored on the online cloud servers, mobile phones or online databases. This data can be hacked easily as it is not encrypted in the transport layer before storing. This enhances the data security risk in IoT system.

2. Inadequate Security Features: With the growing competition and huge demand, technology giants want to launch their IoT software system as soon as soon as possible. Thus the important part of the software life cycle such as testing, quality assurance, and security vulnerabilities are not done properly.

3. Poor mobile security: Poor mobile security in IoT systems make it more vulnerable and risky. Data is stored in a very unsecure way in mobile devices. However, iOS devices are more secure than the Android devices. If a user loses his smartphone and data is not backed up, he will be in a big trouble.

4. Storing data on cloud servers: Storing data on the cloud servers is also considered as a weak link in the security of IoT systems. Cloud servers have less security and are open to attackers from all the dimensions. Developers must make sure that data stored on the cloud servers must always be in the encrypted format.

5. Network attacks: Another big vulnerability in the IoT systems is the wireless connection that is exposed for the attackers. For example, hackers can jam the functionality of a gateway in IoT systems. This can bring down the whole IoT system.

Attacks

Attacks are actions taken to harm a system or disrupt normal operations by exploiting vulnerabilities using various techniques and tools. Attackers launch attacks to achieve goals either for personal satisfaction or recompense. The measurement of the effort to be expended by an attacker, expressed in terms of their expertise, resources and motivation is called attack cost. Attack actors are people who are a threat to the digital world. They could be hackers, criminals, or even governments.

An attack itself may come in many forms, including active network attacks to monitor unencrypted traffic in search of sensitive information; passive attacks such as monitoring unprotected network communications to decrypt weakly encrypted traffic and getting authentication information; close-in attacks; exploitation by insiders, and so on. Common cyber-attack types are:

Physical attacks: This sort of attack tampers with hardware components. Due to the unattended and distributed nature of the IoT, most devices typically operate in outdoor environments, which are highly susceptible to physical attacks.

Reconnaissance attacks – unauthorized discovery and mapping of systems, services, or vulnerabilities. Examples of reconnaissance attacks are scanning network ports, packet sniffers, traffic analysis, and sending queries about IP address information.

Denial-of-service (DoS): This kind of attack is an attempt to make a machine or network resource unavailable to its intended users. Due to low memory capabilities and limited computation resources, the majority of devices in IoT are vulnerable to resource enervation attacks.

Access attacks – unauthorized persons gain access to networks or devices to which they have no right to access. There are two different types of access attack: the first is physical access, whereby the intruder can gain access to a physical device. The second is remote access, which is done to IP-connected devices.

Attacks on privacy: Privacy protection in IoT has become increasingly challenging due to large volumes of information easily available through remote access mechanisms. The most common attacks on user privacy are:

Data mining: enables attackers to discover information that is not anticipated in certain databases.

Cyber espionage: using cracking techniques and malicious software to spy or obtain secret information of individuals, organizations or the government.

Eavesdropping: listening to a conversation between two parties.

Tracking: a users movements can be tracked by the devices unique identification number (UID). Tracking a users location facilitates identifying them in situations in which they wish to remain anonymous.

Password-based attacks: attempts are made by intruders to duplicate a valid user password. This attempt can be made in two different ways: 1) dictionary attack – trying possible combinations of letters and numbers to guess user passwords; 2) brute force attacks – using cracking tools to try all possible combinations of passwords to uncover valid passwords.

Cyber-crimes: The Internet and smart objects are used to exploit users and data for materialistic gain, such as intellectual property theft, identity theft, brand theft, and fraud.

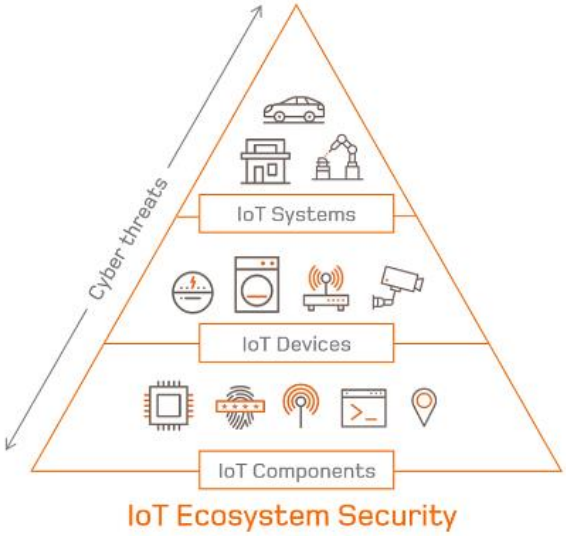
Destructive attacks: Space is used to create large-scale disruption and destruction of life and property. Examples of destructive attacks are terrorism and revenge attacks.

Supervisory Control and Data Acquisition (SCADA) Attacks: As any other TCP/IP systems, the SCADA system is vulnerable to many cyber attacks. The system can be attacked in any of the following ways:

Using denial-of-service to shut down the system.

Using Trojans or viruses to take control of the system. For instance, in 2008 an attack launched on an Iranian nuclear facility in Natanz using a virus named Stuxnet.

III.2. Cyber security and the IoT:



Source: https://www.appluslaboratories.com/global/en/what-we-do/service-sheet/cybersecurity-for-iot-

Making IoT System more Secure

[3] For making secure IoT systems, two things must be kept in mind.

1.Data security: Data security and data mining must be on the top of the list of IoT security features. It is the initial step to prevent any unauthenticated access to the devices in the IoT network. Layered architecture must be used in data security system. Therefore, any breach of initial security level does no expose all the data. Rather it must alarm the authorities about the potential threats and initial level security breach.

2.Authentication: Devices must be secured with the strong passwords for the authentication. Also, third party software security tools can be used that makes devices more secure. This may include bio metrics, facial recognition, speech processing systems etc.

[4]IoT visibility & security in 2019:

1. IoT endpoint security vs network security

Securing IoT devices is a real challenge. IoT devices are highly diversified, with a wide variety of operating systems (real-time operating systems, Linux-based or bare-metal), communication protocols and architectures. On top of the high diversity, comes the issues of low resources and lack of industry standards and regulations. Most security solutions today focus on securing the network (discover network anomalies and achieve visibility into IoT devices that are active in the network), while the understanding that the devices themselves must be protected is now establishing. The fact that IoT devices can be easily exploited makes them a very good target for attackers, aiming to use the weak

[3] https://medium.com/@gunjan.webtunix/internet-of-things-iot-security-risks-and-vulnerabilities-c0729364c809

[4] https://www.cyberdb.co/iot-security-things-you-need-to-know/

IoT device as an entry point to the entire enterprise network, without being caught. Besides that, it's important to remember that network solutions are irrelevant for distributed IoT devices (i.e., home medical devices), that has no network to protect them.

Manufacturers of IoT devices are therefore key for a secure IoT environment and more and more organizations are willing to pay more for built-in security into their smart devices.

2. "Cryptography is typically bypassed, not penetrated" Shamir's law

In recent years we see a lot of focus on IoT data integrity, which basically means encryption & authentication. Though very important by itself, it's important to understand that encryption doesn't mean full security. When focusing mainly on encryption & authentication, companies forget that the devices are still exposed to cybersecurity vulnerabilities that can be used to penetrate the device and receive access into the decrypted information, thus bypassing the authentication and encryption entirely. In other words, what's known for years in the traditional cyber industry as Shamir's law should now make its way to the IoT security industry: "Cryptography is typically bypassed, not penetrated" and therefore companies must invest in securing their devices from cyber attacks and not just handle data integrity. To read more about that, please visit Sternum IoT Security two-part blog post.

3. 3rd party IoT vulnerabilities

One of the main issues in IoT security is the heavily reliance of IoT devices on third-party components for communication capabilities, cryptographic capabilities, the operating system itself etc. In fact, this reliance is so strong that it has reached a point where it's unlikely to find an IoT device without third-party components within it. The fact that third-party libraries are commonly used across devices, combined with the difficulty to secure them, makes them a sweet spot for hackers to look for IoT vulnerabilities and exploit many IoT devices through such 3rd party component.

Vulnerability in third-party components is very dangerous. In many IoT devices, there is no separation and segmentation between processes and/or tasks, which means that even one vulnerability in a third-party library is compromising the entire device. This could lead to lethal results: attackers can leverage the third-party vulnerability to take control over the device and cause damage, steal information of perform a ransomware attack on the manufacturer.

it's not only that third-party components are dangerous, but they are also extremely difficult to secure. Many third-party components are delivered in binary form, with no source code available. Even when the source code is available, it's often hard to dive into it and asses the security level or vulnerabilities inside it. Either way, most developers use the open-source components as black-boxes. On top of that, static analysis tools and compiler security flags lack the ability to analyze and secure third-party components and most IoT security solutions cannot offer real-time protection into binary code.

VXWORKS VULNERABILITIES

A recent example of such third party vulnerability that affects millions of devices can be found in the security bugs found in the VxWorks embedded operating system. These vulnerabilities exposed every manufacturer that used VxWorks operating system, even if security measures like penetration testing, static analysis, PKI and firmware analysis were taken.

To summarize, in order to provide strong and holistic IoT protection, you must handle and secure all parts of the device, including the third-party components. Sternum IoT security solutions focus on holistically securing IoT devices from within and therefore offers a unique capability of embedding security protection & visibility into the device from end-to-end. Sternum's solution is also operating during real-time execution of the device and prevents all attack attempts at the exact point of exploitation, while immediately alerting about the attack and its origins, including from within third-party libraries.

4. Regulation is kicking in

In the past two years, we're seeing a across industries effort to create regulations and standards for IoT security. We are expecting to see more of these efforts shaping into real regulations that will obligate manufacturers to comply with them.

A good and important example is the FDA premarket cybersecurity guidance that was published last year and is expected to become a formal guidance in 2020. The guidance includes different aspects of cybersecurity in medical devices (which is in many cases are essentially IoT devices) such as data integrity, Over-the-air updates, real-time protection, execution integrity, third-party liabilities and real-time monitoring of the devices.

Another example is the California Internet of Things cybersecurity law that states: Starting on January 1st, 2020, any manufacturer of a device that connects "directly or indirectly" to the internet must equip it with "reasonable" security features, designed to prevent unauthorized access, modification, or information disclosure.

We expect to see more states and countries forming regulations around IoT security since these devices lack of security may have a dramatic effect on industry, cities, and people's lives. Top two regulations that are about to be released are the new EU Cybersecurity Act (based on ENISA and ETSI standards) and the NIST IoT and Cybersecurity framework.

Adequate data encryption has three critical steps reviewed below:[5]

1) Understand Your Business and Security Factors
2) Utilize Encryption Protocols Within Your Cloud Architectures
3) Consider Your Encryption Techniques

[5] https://www.iotforall.com/iot-cyber-security/

Thanks to continuous efforts of IT experts in the cybersecurity sector, individuals and enterprises can modify their methods to secure their devices from possible threats. For more guidance, here are other key factors you should know about IoT and network security[6]:

Factor 1: Visibility is everything

In a study conducted by Gemalto in 2019, almost 50% of businesses were able to detect IoT breaches. Again, if it's not visible, it's impossible to measure it; and if it's not measurable, it can be challenging to analyse it and implement possible solutions.

Factor 2: Empower data analysis solutions

Factor 3: Utilisation of new machine learning and artificial intelligence

Factor 4: Implement action plans

Factor 5: Mutual authentication

Security IT developers are now using more advanced cryptographic algorithms. They now include symmetric keys or asymmetric keys when authenticating user access. For instance, the Secure Hash Algorithm or also known as SHA-x can be integrated with a hash-based authenticated code or to the Elliptic Curve Digital Signature Algorithm.

III.3. 10 IoT security incidents[7]

1. Smart Security Cameras

It seems cybersecurity issues with smart security cameras alarmed customers after Xiaomi Mijia's vulnerabilities were exposed. The incident came to light after Dio-V, who owns a Google Nest Hub and several other Xiaomi Mijia cameras around his home, claimed that he received images from other people's homes, randomly, when he streamed content from his camera to a Google Nest Hub.

"When I load the Xiaomi camera in my Google Home hub, I get stills from other people's homes," Dio-V said.

This isn't the first incident where smart security cameras posed an issue.

Ring, a home security products provider owned by Amazon, was hit by a class-action lawsuit in the U.S. for reports of multiple hacking incidents on its security cameras that left victims traumatized.

Security researchers from cybersecurity firm Bitdefender discovered and reported a flaw in Amazon's Ring Video Doorbell Pro, which could have given hackers unauthorized access to the user's Wi-Fi network and potentially to other connected

[6] https://www.iot-now.com/2019/10/29/99666-need-know-iot-cyber-security/
[7] https://www.cisomag.com/10-iot-security-incidents-that-make-you-feel-less-secure/

devices on it. At present, all the Ring Doorbell cameras have received a security patch from Amazon to mitigate the issue.

Also, researchers from vulnerability detection firm Tenable discovered seven critical vulnerabilities in Amazon-owned Blink XT2 security camera systems. If exploited, the vulnerabilities could allow hackers to remotely view the camera footage, listen to audio output, and use the infected device to launch distributed denial of service (DDoS) attacks.

In response, Amazon rolled out patches for the vulnerabilities and urged its users to update their devices to firmware version 2.13.11 or later.

2. Hackers can “Faxploit” Connected Fax Machines

Yaniv Balmas and Eyal Itkin, security researchers from Check Point, discovered that fax machines have security vulnerabilities that could possibly allow a hacker to steal data through a company’s network using just a phone line and a fax number. The researchers also demonstrated how they were able to exploit security flaws in a Hewlett Packard all-in-one printer at DEFCON 26 conference.

Describing the potential threat, the researchers said the attackers can send specially created malware coded image files via fax to the targeted networks. The vulnerabilities in the fax machine enable the malware to decode the files and upload these to its memory, which can breach sensitive information or cause disruption across connected networks.

3. Smart TVs

According to the FBI, smart TVs have several overlooked and neglected security issues. It stated that security is an afterthought for several smart TV manufacturers, which makes them vulnerable to different kinds of threats. Hackers can not only control your unsecured TV for changing channels or volume controls, but also stalk your everyday movements and conversations using the integrated camera and microphone.

4. Smart Bulbs can be Hacked

Multiple reports disclosed security vulnerabilities in smart bulbs. According to Murtuza Jadliwala, a research expert at the University of Texas at San Antonio (UTSA), hackers can compromise infrared-enabled smart bulbs by sending commands via an infrared invisible light emitted from the bulbs to exploit other connected IoT devices existing on the home network.

5. Smart Home is Vulnerable

A Milwaukee-based couple suffered a horrifying incident after their Smart Home setup was hacked by unknown intruders, Fox 6 News reported.

The couple Samantha and Lamont Westmoreland stated that hackers took over their smart home by compromising the connected devices. The attacker played disturbing music from the video system at high-volume while talking to them via a camera in the kitchen, and also changed the room temperature to 90 degrees Fahrenheit by exploiting the thermostat.

Initially, the couple thought it was a technical glitch and changed their passwords, but the issue continued. The duo later changed their network ID, after realizing that someone hacked their Wi-Fi or Nest system.

6. Smartphone's Microphone Can be Used to Launch Acoustic Side-Channel Attack

Academic researchers from England and Sweden designed a malware that can exploit a smartphone's microphone to steal the device's passwords and codes. In their report, "Hearing Your Touch: A New Acoustic Side-Channel on Smartphones," the researchers claimed that they've found the first acoustic side-channel attack that presents what users type on their touch-screen devices.

7. Hackers can Steal Your Identity and Bank Details from a Coffee Machine

Smart coffee machines that are connected to the internet using special apps could be targeted by hackers to steal their owner's bank or card details.

Vince Steckler, chief executive of security giant Avast, said, smart coffee machines allow owners to control them remotely using their phones. Users can even give the machines vocal commands if they are connected to virtual assistant software such as Amazon's Alexa.

"Coffee machines are not designed for security. They are additional vectors to get into your network. And you can't protect them," Steckler said in a media statement.

8. Connected Printers

According to security research firm Quocirca, printers that are connected to an organization's network are the potential vector for cyberattacks. In its report, "Global Print Security Landscape, 2019," Quocirca addressed the potential security vulnerabilities posed by connected printers.

The report highlighted that 60 percent of businesses in the U.K., U.S., France, and Germany suffered a print-related data breach in 2019, which resulted in a data loss that cost companies an average of more than US$ 400,000.

9. Smart Speakers Can be Hacked

Wu HuiYu and Qian Wenxiang, security researchers from Tencent Blade, exposed vulnerabilities around smart speakers in a live demonstration at the DEFCON security conference on how to hack a smart speaker. The team used Amazon Echo smart speakers to present their attack program.

The researchers hacked the speaker by adding a malicious device embedded with an attack program. They also notified their findings to Amazon before the presentation, and Amazon pushed a security patch to fix the issues.

10. Even Internet-Connected Gas Stations are Vulnerable

Researchers at Trend Micro discovered that hackers are targeting internet-connected gas stations to launch IoT-based cyberattacks.

In its report, "The Internet of Things in the Cybercrime Underground," Trend Micro described how Russian hackers have benefited from the Russian government's new directive, which mandates to replace all electricity meters in the country with smart meters. Trend Micro stated that hackers in Russian dark web forums requested information on how to exploit smart meters. Some hackers are even selling altered smart

meters in the underground market forums. Researchers also revealed that they've seen tutorials on gas pump hacking, including step-by-step procedures on how to hack connected meters.