Deisithani.S

HAZARDS AND SAFETY REQUIREMENTS OF INTERNET OF THINGS (IOT)

The Internet of things (IOT) is taking the concept of safety to a whole new level. In a world where everything can be connected, and physical contact becomes optional, verbal instructions and even facial recognition are used to operate the end device, safety considerations must be made.

There are two categories of safety hazards associated with the IOT:

- Type 1 hazards are directly associated with the traditional use of the device and include things such as: overheating, shock, sonic hazards, etc. Introducing IOT into products could increase the frequency of occurrence of these hazards. Enabling remote operations means that hazards of these kinds are no longer bounded by physical limitations. For instance, an electronic oven that can be turned on and off remotely can become hazardous if a faulty command is received when no one is present to watch it.
- Type 2 hazards are indirectly related to the device and its operation but could enable a security or safety issue by implementing IOT. The cascade effect could be a breaching of properties or leakage of private information. Imagine a snowy winter in the north eastern U.S. where a smart garage door opener fails and starts to open while the family is away for vacation. The property is exposed to severe weather, whereas a hardwired garage opener will more likely to stay closed during a failure.

Newly developed regulations and standards address the above hazards properly by recognizing the root cause of these hazards and the unseen applications for existing products. One leading sector is home appliances. At present smart cooking, lighting and temperature control are the frontline of IOT safety candidates. Drones and similar devices with the capability of injuring people or damaging financial assets must also be considered. Autonomous vehicles are being produced widely and IOT-enabled devices for the automobile industry are emerging, bringing another layer of safety concerns to driving hazards.

It is expected that IOT safety evaluation will be closely coupled with functional safety, which was established at the end of the 20th century for industrial environments. International and regional standards include: IEC61508

series, ISO26262 series, ISO12100, ISO13849 series, IEC60730-1 series, UL5500, CSA Z434 series, ANSI B11 series.

Key aspects related to functional safety evaluation include:

- Planning and design elements
- Risks and hazards
- Management plans
- Performance Levels (PLs)
- Safety Integrity Levels (SILs)
- Failure modes, effects, and diagnostic analysis (FMEDA)
- Designated personnel responsibility
- Rigorous documentation
- As the IOT continues to evolved, it's important to stay informed about risk and safety standards to help make sure products meet regulatory requirements and the demands of consumers. It could be the key to success.
- *Ang Zhu is an engineering lead at Intertek's Cortland New York facility, where he is responsible for certifying power generation and conversion equipment, functional safety consultation, researching new standards and technologies, and providing regional and global technical support and guidance. He is a committee member of IEC 61508 TC 65 and E.I.T in New York State. He received a bachelor's degree from South China University of Technology (SCUT) and master's degree in Electrical Engineering from both SCUT and New York University Tanon School of Engineering.*

Most Common Internet of Things (IOT) Security Risks

Attack surfaces, threat vectors and vulnerabilities are three widely researched topics when it comes to the Internet of Things (IOT). There are a variety of dangers related to the internet of things that can impact businesses as well as individuals. We will describe 11 of the most common Internet of Things security risks so that you can take steps to protect your business and its stakeholders.

The Most Important Security Problems with IoT Devices

- Incorrect access control.
- Overly large attack surface.
- Out dated software.
- Lack of encryption.

- Application vulnerabilities.
- Lack of Trusted Execution Environment.
- Vendor security posture.
- Insufficient privacy protection.

Increased attack surface

Every connection that can be made to the device allows an attacker to potentially discover and exploit vulnerabilities. The more services a device offers, the bigger the attack platform becomes. Offering unnecessary or unneeded services over the Internet can potentially compromise confidentiality, integrity and availability of that information.

No or weak encryption

Devices with lax security often communicate in plain text. This means that sensitive information like API tokens or credentials can be obtained through a “Man in the Middle” (MITM) attack. A MITM attack is where an attacker secretly accesses and relays communications, possibly altering this communication, without either party being aware.

Weak physical security

Security for IOT devices is not about digital security, physical security also represents a significant risk. Consumer and industrial IOT devices often store sensitive information. Information used as passwords of wireless networks is connected to or event sensitive video or audio information related to the company, home, or user(s).

With physical access to the devices, attackers can open them and bypass security software by reading the contents of the memory components directly.

Bad privacy protection

Consumer IOT devices often store sensitive information. For example, any wireless IOT device will store the password of that network. Any IOT device that records video or audio likewise potentially contains information related to a company, home, or user. In case such information is available to an attacker, it would be considered a privacy violation. IOT devices can properly and securely handle private information.

Application vulnerabilities

Software contains bugs that make it possible to trigger unintended functionalities. These vulnerabilities can result in security issues. Also, the lack of the ability to securely update the device can introduce vulnerabilities. When looking for an IOT device provider it pays to find a vendor that focuses on continued support and security.

Lack of trusted execution environment

Essentially IOT devices are small computers and have the capability to run most types of specific software. This allows attackers to perform the installation of custom made software that is not part of the device's normal functionality. For example, an attacker could install software that allows him to perform a denial of service attack (DDOS). It is essential to limit the functionality of IOT devices to deter abuse.

Vendor security

Security support is needed for I OT devices to maintain a proper security composure. Lack thereof could cause a wide variety of security issues. When vulnerabilities are found regarding an IOT device, it is essential to have the vendor develop mitigation and update the devices in the field as soon as possible. The vendor should have a process in place to adequately handle such issues**.**

Lack of intrusion awareness

Most devices do not have any logging or alerting features to notify users of security issues. Changes in power or bandwidth usage are usually not detected or reported to the user, which is typically a way of identifying a compromise. Those devices with these reporting and alerting functionalities can usually be easily disabled when the device is compromised.

Weak passwords

Weak passwords selected by the user or vendor, and device hardcoded passwords that cannot be changed, also represent a significant security risk. Use unique passwords for your devices, make them at least 12 characters long, use numbers, symbols, and letters (upper and lower case). Adopting a good policy towards what represents a strong password will greatly reduce the chance of the password being guessed or brute-forced.

Out dated software

Using out dated, depreciated or insecure software components can allow an Internet of Things (IOT) device to be compromised. This includes the usage of third-party components, libraries, and frameworks used by manufacturers to build IOT devices. This software is difficult to track and is vulnerable to cyber attacks if it is not correctly known or managed.

When choosing your IOT device you should consider more reputable suppliers with a strong focus on security, not just the cheapest option. Cheap products usually mean out dated, vulnerable software.

Conclusion

From an IOT security standpoint, it is important to incorporate IOT security into security policies, procedures and guidelines. It is vital to assume that every IOT device needs configuring after initial deployment. Knowing your device is critical. Deploying proper authentication mechanisms and strong password policies is needed, as well as proper update and patch management.

When it comes to the security of your home and organisation, you should do your best to ensure that it is at a sufficient level. You can't always rely on the IOT device supplier. Since Internet of Things devices are rapidly taking over our world, more awareness and know-how is needed to incorporate IOT security into our daily lives. We hope this article has given you a good idea of the most common security risk associated with IOT devices.