IoT Vulnerabilities and the IoT Security Crisis

kajeet®

The number of connected IoT devices is growing rapidly. From cars, light bulbs, and electric outlets to medical equipment, industrial machines, and home appliances, smart devices are making their way into many parts of our daily lives.

Embedded sensors that allow these devices to communicate with other devices and computer systems via the Internet have valuable applications in education, transportation, finance, logistics, agriculture, utility management, building automation, and more, and these applications are what have driven a new wave of adoption and growth in the IoT space.

While IoT devices can power a broad new set of capabilities, the rapid diffusion of connected smart devices across many different verticals and industries comes with many serious security implications. Smart devices and embedded sensors must be protected and regularly maintained – preferably proactively before an attack can occur, rather than reactively – and there are many other steps that businesses and organizations must take to secure their devices, data, and IT processes from attack.

In the sections below, we talk about what security means, what can make IoT devices vulnerable, how these vulnerabilities can affect users, and how to secure your devices, networks, and applications.

What Does Security Mean?

What are we talking about when we say "IoT security"?

The first thing to understand is that IoT systems can be attacked on many fronts and in a variety of ways. For example, a physical attack may involve unauthorized access or tampering with hardware components. Denial of Service (DoS) attacks aim to make a device or network resource unavailable to its users. Access attacks, privacy invasions, data mining, cyber espionage, eavesdropping, tracking, and various forms of cybercrime (the exploitation of users and data for materialistic gain) are all serious issues with which IoT network operators and device manufacturers must contend. TCP/IP (used to connect to the Internet) and SCADA systems (used in industrial settings) are also vulnerable to DoS attacks and Trojans, malware, and viruses. When we talk about security, we mean securing your devices and systems from these types of attacks.

Key Security Goals

Before implementing or adopting specific IoT security measures, it is worthwhile to first outline what your broad security goals are. From there, you can develop a robust system that addresses the issues and/or threats you face.

In general, IoT security aims to protect your systems, data, and devices from the attacks above to prevent issues in the following areas:

Confidentiality: Maintaining confidentiality is crucial, especially when dealing with data that might be sensitive, such as healthcare/patient data, private business information, military data, security credentials, and financial data.

Integrity: You must ensure data integrity, which is different from ensuring confidentiality and privacy. Ensuring integrity means that you are able to flag errors in data recording and identify when potential manipulation may have occurred.

Authentication and authorization: IoT systems operate under what is called ubiquitous connectivity. In such systems, communication can take place around the clock between devices and/or humans. Different systems require different authentication protocols based on the use case at hand or the users or applications involved.

Availability: Devices and users must be able to access information and services when they need them – without interruption. Downtime can lead to serious issues, from a loss of trust to financial losses and even the loss of life, as can occur in healthcare IoT systems or fire monitoring in building automation systems.

Auditing: What criteria should you use to evaluate your security, and when and how will remedial steps be executed? Security system audits are systematic evaluations of your network, devices, and applications against a set of predetermined criteria, and they allow you to identify and then patch potentially exploitable weaknesses. The kinds of audits you need to use will depend on the applications, data, and device types connected to or running on your networks.

What Makes IoT Devices Vulnerable

Many IoT devices and systems run on networks or use devices that lack the built-in security required to repudiate threats.

Here are a few examples of vulnerabilities that can enter your system:

Hardware limitations and limited computational power: Many IoT devices are only designed to perform an array of specific functions. To lower power consumption and data transmission needs, many devices are designed with only the most basic features and components in place – leaving little room for security and data protection mechanisms.

Dissimilar transmission technologies: Different devices, networks, applications, and infrastructures can use different transmission technologies such as 2G, 3G, 4G, 5G, Wi-Fi, CDMA, LTE, and more. This can make it hard to establish robust and thorough protection standards across all network endpoints (not to mention the protocols and software that run on them).

User issues: A lack of user security awareness can expose smart devices to attacks. Weak, guessable, and default passwords are examples of user-related issues that can lead to system breaches. Weak passwords can be guessed using brute-force attacks. They may also be publicly available or even unchangeable. Social hacking and the intentional, unauthorized sharing of access credentials are also examples of user issues that can compromise your network.

New legislation, such as California's Senate Bill 327 (approved in 2018), prohibits the use of default certificates with IoT devices and is a legal solution to the issue of weak passwords.

Here are a few additional examples of vulnerabilities that may creep into an IoT system.

- **"Weak link" in the network:** Networks are only as strong as the weakest link, device, node, application, or interface connected to the network. A failure to secure devices, interfaces, or applications can lead to lateral movement within a system if a hacker can gain entry via an unsecured or vulnerable application or interface.
- **Not receiving regular system updates:** You must ensure that your devices can receive regular over-the-air (OTA) updates that can help minimize your attack surface across your applications, firmware, and operating systems. These updates may quickly and easily secure devices, validate firmware, secure the delivery of information (which must be encrypted during transit), and generate notifications of security issues that may arise along with such updates.

Without them, you will be inherently exposed to attacks. Some devices may have reached the end of their useful life, and others may not be upgradable to begin with.

- **Device management issues:** You must provide deployed devices with active security support. This requires asset and update management, timely (and secure) decommissioning, and 24/7/365 systems monitoring. You must also manage device identities, risk profiles, and permissions. These measures can prevent rogue or malicious devices from being installed on an otherwise secure network without the requisite approvals or authorizations.
- **Insecure data transfer and storage:** The data within your system data must be encrypted and protected by access control protocols anytime it is in storage, is in transit, or is being processed.
- **Insecure network services:** Unnecessary or unsecured services that run on IoT devices can jeopardize data and/or system availability, confidentiality, and authenticity. Vulnerable ports

must be closed, but monitoring and managing ports can be challenging, which is why many enterprises fail to do it.

- **Insecure interfaces:** Data travels between web applications, backend APIs, cloud hardware and applications, and mobile interfaces and applications. Therefore, data transfer between devices, sensors, gateways, and back-end databases via REST-based APIs must be secured and encrypted.
- **The use of insecure or outdated hardware or technologies:** Outdated or insecure software libraries or devices can expose your IoT network to attacks. Outdated legacy systems, third-party components or libraries and frameworks that have not been tested, and poor QA/QC practices can lead to unauthorized access of your network or devices.
- **Inadequate privacy:** It can be difficult to tell if an IoT device is gathering user data – and what kinds of data it may be collecting. If a user wishes to delete his or her data, providers must ensure that all third parties delete that data as well.
- **Insecure default settings:** Devices may be accessible while they are being onboarded (i.e., added or connected to a system) with default manufacturer passwords or settings in place. External parties can potentially eavesdrop during onboarding to intercept keys or passwords that will then be used to gain network access.
- **A lack of physical hardening:** Many IoT devices are installed or deployed in remote areas and may not be regularly surveilled or monitored, allowing hackers to gain access to network-connected devices via physical access to the device. Although many IoT devices use various security protocols to protect data while data is in transit, many do not protect data that is stored on the device itself. Data breaches from physical access can also result should a device be stolen or if discarded equipment falls into the wrong hands. Trusted Platform Modules (TPMs) or Trusted Execution Environments (TEE) can be used to store keys or sensitive data to prevent physical access breaches of your devices.

How Vulnerabilities Affect Users

Once a hacker gains entry to a system, they may be able to move laterally to other systems and devices. Compromised devices can also be weaponized to spread malware to the rest of your network or to launch botnet or DoS attacks that can lead to a lack of service availability.

For example, IoT devices at home can lead to intrusion in work networks from compromised home devices or appliances (an important consideration in work-from-home and bring-your-own-device arrangements). Also, hijacking uncommon targets such as HVAC systems or wearable health devices such as insulin pumps can have unexpected and undesirable long-term consequences. Home intrusion, identity theft, financial crimes, crypto-jacking, and the theft of sensitive or private data are all examples of how a data breach can affect businesses and private individuals.

Effectively securing the diverse range of devices on your network requires a multi-layer security plan.

How to Secure Your IoT Networks and Devices

Securing your devices and networks depends on the kinds of devices and networks you have, as well as the software, applications, and data that run on them. Effectively securing the diverse range of devices you likely have on your network requires a multi-layered security plan.

Here are five steps that organizations can take to start ramping up IoT security:

- Change default passwords and adjust security settings, permissions, access, visibility, and discoverability as required.
- Turn off or disable features or services that you do not need.
- Only use legitimate third-party applications from valid vendors.
- Update device firmware and applications and automate secure updates.
- Review and audit device logs and permissions (asset management).

Once you have completed the above, you can move on to securing network devices and routers as follows:

- Map and regularly monitor all of your connected devices, including their settings, credentials, firmware versions, and recent patches.
- Apply network segmentation to contain an attack should one occur.
- Make sure that your network architecture is secure by setting up your routers using VLAN segmentation, isolation, and firewalls.

Shifting from Reactive to Proactive Network and Device Security

IoT devices and systems tend to be designed with ease-of-use, cost savings, extended battery power, and minimum maintenance prioritized over security. As such, these devices are often unable to detect potential issues such as unauthorized access or malicious activity. This design, combined with the data that they generate and/or transmit, makes them easy and lucrative targets. Also, some IoT devices work with obsolete or legacy operating systems that cannot be patched, so security is understandably a big concern.

Here are six steps you can take to improve your IoT security strategy.

1

SYSTEM, PROCESS, & DEVICE VISIBILITY IS KEY

First, you must take an accurate and up-to-date inventory of all of the devices and systems in your network. To do this, you can use deep packet inspection on a network TAP (test access point), which will evaluate packets that are transmitted through the inspection point in your network to remove security protocol non-compliance as well as spam, viruses, malware, and any data that you want to remove. You can also use SPAN (port monitoring) to do the same. These processes will give you the information you need to enjoy in-depth system visibility, such as the make, OS, serial number, classification, and application or port usage of all devices.

2

UNDERSTAND DEVICE BEHAVIORS & PERMISSIONS

You must have insight into how all network and system devices behave and what parts of the network they can or are communicating with.

3

CENTRALIZE MANAGEMENT

Use a single dashboard to track and investigate at-risk devices. This will help with asset management, maintenance, and configuration.

The Kajeet Sentinel® platform is an innovative cloud-based portal allowing administrators full IoT device and data management. Learn more about how Sentinel can benefit your connected IoT system.

https://www.kajeet.net/products/

4

SEGMENT YOUR NETWORKS

Segmentation can be used to control and, if necessary, isolate at-risk or compromised device connections or processes.

5

ESTABLISH CONTINUOUS MONITORING

Your IoT network needs real-time notifications of new devices, potential vulnerabilities, and threats. The challenge of managing a ransomware attack as soon as it occurs highlights the importance of continuous monitoring of network-connected devices and proper baselining and segmentation.

6

AUTOMATE INCIDENT RESPONSE PROTOCOLS

Create and enforce segmentation policies that are used to mitigate or remove threats based on alerts or trigger-specific events.

These steps can help you address potential vulnerabilities, threats, and risks and help you manage your IoT devices wherever they are in your network.

Conclusion

You need to understand your systems, devices, and networks, as well as where and how they may be vulnerable before deploying IoT security measures. Your IT teams should consider how the data and devices you use – and the products and services you provide – interact with the hardware, software, network points, and applications that make up your IoT network. From early intrusion detection and automating incident response to system architecture, device design, physical security, and worker training regarding security best practices, there are many ways you can secure your networks and devices from costly intrusions and unauthorized access.

To learn more about how we can help you deploy an IoT system that protects your devices and networks, contact a Kajeet Security Specialist today at **www.kajeet.net/contact-us/.**