## **What are the Challenges of IoT Security?**

IoT has many of the same security challenges that other systems have. There are, however, some challenges that are unique to IoT.

1. Embedded Passwords. Embedding passwords in IoT devices make it easy for remote support technicians to access devices for troubleshooting and simplifies the installation of multiple devices. Of course, it also simplifies access to devices for malicious purposes.
2. Lack of device authentication. Allowing IoT devices access to the network without authenticating opens the network to unknown and unauthorized devices. Rogue devices can serve as an entry point for attacks or even as a source of attacks.
3. Patching and upgrading. Some IoT devices do not provide a simple (or any) means to patch or upgrade software. This results in many IoT devices with vulnerabilities continuing to be in use.
4. Physical hardening. Physical access to IoT devices can introduce risk if those devices are not hardened against physical attack. Such an attack may not be intended to damage the device, but rather to extract information. Simply removing a microSD memory card to read its contents can give an attacker private data, as well as information such as embedded passwords that may allow access to other devices.
5. Outdated components. When vulnerabilities are discovered in hardware or software components of IoT devices, it can be difficult and expensive for manufacturers or users to update or replace them. As with patches, this results in many IoT devices with vulnerabilities continuing to be used.
6. Device monitoring and management. IoT devices do not always have a unique identifier that facilitates asset tracking, monitoring, and management. IT personnel do not necessarily consider IoT devices among the hosts that they monitor and manage. Asset tracking systems sometimes neglect to include IoT devices, so they sit on the network without being managed or monitored.

Most of these issues can be attributed to security being an afterthought (if a thought at all) in the design and manufacturing of IoT devices. Even those IoT developers who consider security in the design process struggle with implementation. Most IoT devices are limited by minimal processing power, memory, and data transfer speeds. This is a necessary evil in order to keep the size and cost of the devices small. Accordingly, security controls must be implemented to compensate for these inherent weaknesses.

The first step to implementing security controls is to determine where those controls are needed. This is another challenge for protecting IoT devices. Since IoT devices are often not recognized as network devices, they get overlooked when inventorying or mapping the network. If you do not know it is there, you cannot protect it.

Fortunately, IoT device manufacturers are beginning to address these issues, but organizations that are planning or currently using IoT cannot sit back and wait for that to happen. There are measures that organizations can take right now to protect their IoT devices and networks from attacks.

## Security Requirements of IoT

Manufacturers and implementers must implement security practices to mitigate IoT risks. Steps can be taken to better secure IoT and address known risks.

|  |  |
| --- | --- |
| **Security Challenge** | **Solution** |
| Embedded passwords | Rather than embedding passwords in their products, manufacturers should require users to create a strong password during device setup. |
| Lack of device authentication | Manufacturers should provide a means for their devices to authenticate to the network. IT personnel should require devices to authenticate before joining the network. |
| Patching and upgrading | Manufacturers need to make it easy for devices to be upgraded or patched. Ideally, this would be an automatic or one-click process. |
| Physical hardening | IoT devices should be made tamper-proof. Devices should be monitored to detect time offline and inspected after unexpectedly dropping offline. |
| Outdated components | Vulnerable devices should be updated or replaced. This can be difficult to remedy, especially in environments that have many IoT devices in remote locations. In those cases, tighter security controls and more vigilant monitoring should be implemented. |
| Device monitoring and management | Ensure that all IoT devices are included in asset tracking, monitoring, and management systems. Manufacturers should provide a unique identifier for each device. |

Clearly, many of these security issues can only be resolved by the manufacturer. One that organizations’ security, IT, and OT teams can address is device management. It is up to those planning and/or implementing the rollout of IoT devices to ensure that they are accounted for in asset management, systems monitoring, security monitoring, and incident response systems.

## Breaches and Hacks

There are two broad categories of attacks that involve IoT devices: those in which the IoT devices themselves are the end target of the attack, and those that use IoT devices to attack other targets. We have seen both types of attacks used in the real world and by security researchers as a proof of concept.

In October of 2016, [an attack against Dyn](https://www.forbes.com/sites/davelewis/2017/10/23/the-ddos-attack-against-dyn-one-year-later/#3a47f1581ae9), a company that provides DNS services, made much of the internet inaccessible. Twitter, Spotify, Github, Netflix, The New York Times, Paypal and other major websites were down for hours.

The attack used the Mirai IoT Botnet, taking control of over 600,000 IoT devices to flood Dyn with traffic in a massive DDoS attack. The devices seemed to be mostly routers and IP cameras. IP cameras are frequently targeted IoT devices.

In a scary example of an attack where the IoT device was the target, the “device” was a car. Fortunately, this was a controlled demonstration by security researchers Charlie Miller and Chris Valasek. They demonstrated the attack for [Wired](https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/) writer Andy Greenberg, who was driving a Jeep Cherokee.

Miller and Valasek, from miles away over a cellular internet connection, remotely turned on the A/C, radio, and windshield wipers. That was just the beginning. Next, they caused the Jeep to slow, remotely rendering the accelerator useless.

## How to Secure IoT Systems and Devices

It is clear that IoT attacks can have serious consequences. Securing IoT systems and devices must be done by both the manufacturers and the organizations using them. The security controls that organizations can put in place are similar to the controls they already use on their network. The key to securing IoT is to know what IoT devices are on your network and where they are in your network topology. Until you know that, you are flying blind. You cannot protect what you cannot see.

One way to identify IoT devices on your network is to require all hosts and devices to authenticate when joining the network. Devices that fail authentication can then be identified. If they belong on the network, authentication can then be configured for that device. If they do not belong on the network, you have discovered a rogue device.

You can further secure IoT devices by segmenting the network and dedicating one segment to IoT. This will allow you to firewall that segment and apply IoT-specific rules. It would also allow you to quickly block traffic from that segment in the event that an IoT device is compromised.

Once you have IoT devices authenticated, you can then gain visibility into their activity using a cloud-native security monitoring and analytics platform like [Sumo Logic](https://www.sumologic.com/solutions/security-analytics/). The Sumo Logic platform helps you make data-driven decisions and reduce the time to investigate security and operational issues so you can free up resources for more important activities. For even greater visibility into security events, [integrated threat intelligence](https://www.sumologic.com/application/integrated-threat-intelligence/) from Crowdstrike is included for up-to-date IOC data that can be quickly cross-correlated to identify threats in your environment.

**Reference:** <https://www.sumologic.com/blog/iot-security/>