HC3: Analyst Note
August 04, 2022 TLP: White Report: 202208041700

Internet of Things (IoT) Security

Executive Summary
The Internet of Things (IoT) describes the network of physical objects that are installed with sensors, software, and other technologies to connect and exchange data with other devices over the internet. These devices can range from everyday household objects to industrial tools. Today, there are about 7 billion devices connected through IoT and it has been estimated that devices using this technology will increase 20 billion more by 2025. While IoT has existed for a while, advancements in technology have made it more practical and accessible. There is an increase in security concerns that exist with this technology along with the many organizations that operate them such as healthcare, finance, manufacturing, logistics, and retail. It's architecture typically consist of wireless networks and several components to exchange data. While IoT projects can differ, the main architectural layers have remained consistent. With the increased use of this technology there also comes concerns to an increase in cyber-attacks on it. Distributed Denial of Service (DDoS) or Man In the Middle Attacks (MITM) are some of the common exploits used against the IoT. Additionally, adding IoT to an organization can increase the attack surface on which a company can be vulnerable if the network isn't sectioned off into secure zones. Like all objects connected to the internet they're ways to help secure these devices ranging from good physical security and ensuring the firmware is updated regularly.

Report
The IoT is a physical object that can connect to the internet. Connecting all these different objects and adding sensors to them adds a new level of intelligence that enables them to communicate in real-time. The Internet of Things is making the world around we live in more responsive by merging the digital and physical universes.

Common IoT Uses
Smart Homes: IoT can be used to monitor, control appliances, and manipulate our environment including temperature, lighting, entertainment, and other smart devices.

Healthcare: Medical IoT (MIoT) is providing healthcare professionals the ability to monitor patients with smart devices that can track blood pressure, heart rate, and glucometers.

Smart Cities: Data from smart devices is also benefiting cities by allowing workers to gather information on lights, meters, waste, and even air quality.

Vehicles: Vehicles connected to the internet allows users to access data to the cars maintenance and it can enable the ability to electronically pay tolls.

Fitness Trackers: Mostly used for healthcare and sports. These devices allow users to find their blood pressure, heart rate, and other metrics associated with physical activity.

The Importance of IoT Security

Any device connected to the internet has the potential to be hacked and the Internet of Things is no exception. A compromise of these devices could lead to devasting damage including tampering with traffic lights, shutting down home security systems, and damage to human life. Since these devices can collect data to include personally identifiable information it is important to secure these systems. Ultimately, the goal is to protect the entire system, but there are steps that can be taken to help accomplish this.

1. Securely store, process, and transfer data
2. Keep the device safeguarded
3. Update the device to reduce vulnerabilities

Limiting the Attack Surface on IoT

With the implementation of IoT technology in an organization users are also widening the attack surface on which they can become a target from threat actors. Having IoT, IT devices, and operational technology (OT) in the same network is commonly reffered to as a flat network. The main vulnerable in this is that once attackers gain inital access, they can perform lateral movement and compromise more sensitive systems. Incorporating network segmentation is a good way to limit the attack surface and prevent entire systems from being compromised.

Network segementation is a component of cyber security that is designed to prevent the spread of malware to other OT and applications. In network segmentation, the network is split into multiple subnetworks or zones which can also reduce congestions and limit failures. This way the IoT devices are isolated from other IT equipment in use. Organizations operating with no segmentation are at a greater risk of being compromised.

Common IoT Attacks

Privilege escalation: Attackers can exploit bugs, unpatched vulnerabilities, design flaws, or even operating systems in an IoT device to obtain unauthorized access.

Man-in-the-Middle (MITM) Attacks: A type of attack where an actor can intercept information being sent between two parties. This can also be used to steal or alter data.

Eavesdropping: This can occur when an attacker intercepts, deletes, or modifies data that is transmitted between devices. This attack relies on unsecure network communications.

Brute-force attacks: Many IoT devices are left unchanged with factory set passwords. Threat actors can execute brute force attacks to gain access.

Firmware hijacking: Each device has software, updates, and modifications. Actors can take advantage of this environment by adding fake updates or drivers to download malicious software.

DDoS: When infected with botnet malware, IoT devices can be used to perform large scale cyber-attacks.

Physical tampering: Threat actors could gain initial access from physically insecure IoT devices to install malware.

Minimizing Risk from IoT Devices

Change default router settings: Most people do not rename their router and keep the manufacturer's default settings. Make sure to change the privacy and security settings on new devices. Those settings typically benefit manufacturers more than the user.

Pick a strong password: Strong and unique passwords are a great defense against hackers. Make sure to use a secure password for each device. If multiple devices are using the same password than one compromised device can lead to actors accessing more of them.

Avoid using Universal Plug and Play: Universal Plug and Play (UPnP) makes it easier to network devices without additional configuration. This feature can also make office equipment vulnerable to cyber-attacks.

Keep your software and firmware updated: Firmware keeps you protected with the latest security patches and reduces the chances of cyber-attacks. You can fix vulnerabilities or exploits as they emerge and secure your IoT devices by updating its software.

Implement a Zero Trust Model: A zero trust model assumes that nothing can be trusted in or outside of the network. Every organization has a variety of users, but only a limited amount of people require access to certain resources to accomplish their job. For this strategy to be effective administers must determine who the users are and what role they play in the organization.

References

Fortinet. "Eavesdropping" https://www.fortinet.com/resources/cyberglossary/eavesdropping

Katrenko, Anna. Semeniak, Elena. "Internet of Things (IoT) Security: Challenges and Best Practices"

apriorit. 17 Feb, 2022. https://www.apriorit.com/dev-blog/513-iot-security

*Kulkarn, Swamini i . "*How to secure IoT devices and protect them from cyber attacks" Techtarget. 08 July, 2021. https://www.techtarget.com/iotagenda/post/How-to-secure-IoT-devices-and-protect-them-from-cyber-attacks

MongoDB. "What is IoT Architecture" https://www.mongodb.com/cloud-explained/iot-architecture

Oracle. "What is IoT?" https://www.oracle.com/internet-of-things/what-is-iot/

Ranger, Steve. "What is the IoT? Everything you need to know about the Internet of Things right now" ZDNet. 03 February, 2020. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

Socradar. "Common IoT Attacks that Compromise Security" 13 May, 2022. https://socradar.io/common-iot-attacks-that-compromise-security/#:~:text=Privilege%20escalation%3A%20Attackers%20could%20exploit,unauthorized%20access%20to%20the%20network.

TrendMicro. "IoT Security Issues, Threats, and Defenses" https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

Newton, Peter. "Simplify zero-trust implementation for IoT security" TechTarget. 13 May, 2022. https://www.techtarget.com/iotagenda/post/Simplify-zero-trust-implementation-for-IoT-security#:~:text=The%20zero%2Dtrust%20model%20is,means%20an%20expanded%20network%20perimeter.

Kerravala, Zeus. "How network segmentation provides a path to IoT security" networkworld. 17 Dec, 2015. https://www.networkworld.com/article/3016565/how-network-segmentation-provides-a-path-to-iot-security.html

Rosario, Mayra. Huq, Numaan. "Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risk" Trendmicro. Securing Connected Hospitals: A Research on Exposed Medical Systems and Supply Chain Risks (trendmicro.com)

Nozomi Networks. "New OT/IoT Security Reports: Trends and Countermeasures for Critical Infrastructure Attacks" Automation. 07 Feb, 2022. New OT/IoT Security Report: Trends and Countermeasures for Critical Infrastructure Attacks (automation.com)

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback