PONDURANCE

Security As a Foundation for IoT



pondurance.com



Introduction

While almost every modern electronic device connects to the cloud, they are often not designed with security in mind. The Internet of Things (IoT) is an exciting environment with use cases ranging from self-driving cars to surveillance cameras to heavy machinery to smart garbage cans. Despite the amazing opportunity of IoT, none of the potential gains will be realized if the devices, communications, and data are not secured. Security must be a pivotal piece of the design of any IoT implementation and must be thought of as a foundation of the overall solution.

What Is IoT?

IoT is a growing system of billions of devices that connect through wireless networks to the internet and each other. IoT can be found in consumer products, commercial and industrial devices, and even the military. Primary examples include:

CONSUMER IoT

Home use (e.g., smart baby monitor)

COMMERCIAL IoT

Business use (e.g., internet-connected heating, ventilating, and air conditioning (HVAC) unit)

INDUSTRIAL IoT (IIoT)

Manufacturing use (e.g., systems controlling robots at a factory)

INFRASTRUCTURE IoT

Specific to energy, water/sewer, or other utilities (e.g., smart electric meters)

MILITARY IOT (IoMT)

Specific to military use (e.g., unmanned warfare)

127 NEW DEVICES
are connected to the web every
SECOND



MORE THAN
75 BILLION
IoT devices expected
TO BE CONNECTED BY 2025[1]

PONDURANCE

Types of Vulnerabilities

IoT device vulnerabilities are particularly concerning because a compromise could have a detrimental outcome outside of the digital environment. For example, an attacker could access an HVAC system and overheat it. Below are the types of vulnerabilities to keep an eye on.

PHYSICAL VULNERABILITIES INCLUDING:

- Weak, guessable, or hardcoded passwords.
- Insecure network services
- Lack of hardening, device management, and/or privacy protection
- Unused ports-both physical (e.g., uArt or RS232) and virtual (superfluous services)

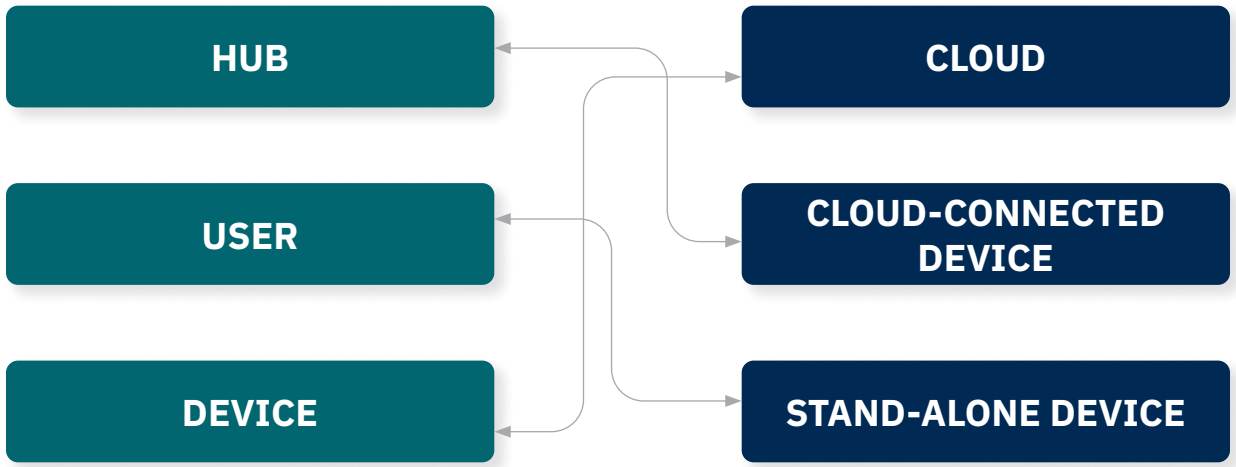
FIRMWARE VULNERABILITIES INCLUDING:

- Conventional vulnerabilities like programming errors.
- Stored security keys.



Common Network Attack Vectors

Networking in IoT is a very complex, tangled web of mesh networks, where devices connect to other devices that connect to other devices. There are many combinations of potential connections, and an attack can target communications between any of the following:



PONDURANCE

How To Protect Your Data



DATA IS ABUNDANT IN IOT DEVICES SO IT IS IMPORTANT TO CONSIDER EVEN MORE PROTECTIONS:

- Clever log and network monitoring is needed because many IoT endpoints do not keep logs and network communications are often unrestricted. Any design plan for an IoT solution should define logging practices and profile network communications to more easily detect deviations from standard endpoint profiles.
- As always, it is key to consider CIA for data (confidentiality, integrity, availability):
  - **C:** Only those with permission can read the data (protects against data theft).
  - **I:** Only those with permission can modify the data (protects against data modification).
  - **A:** Those with permission can always access the data (protects against data loss).
- Special protections around precision and accuracy of data are needed because real-time decisions are being made based on the data. In a widely known example, Boeing 737 Max experienced an unbounded loss of data accuracy. With limited plans in place to address this loss of accuracy, the result was tragic.
- Privacy and human rights will play a big role in IoT security, but it remains to be seen how — as the amount of potential IoT data dwarfs the personal data available on the internet — protecting that data will be front and center.

Conclusion

The IoT is an incredible platform for innovation. However, IoT will continue to open opportunities for new online threats. As with any new technology, strong security is essential. A standardized approach is needed based on established principles to ensure it is as secure as possible.

We recommend establishing tools and programs in alignment with the NIST Cybersecurity Framework.[2] It is also key to have prevention, detection, and response plans in place such as those MDR service provides. Most importantly, having a disaster response plan is key, and not just for hacks but also for business situations where malfunctioning IoT or inaccurate data would cause damage like the Boeing 747 Max case. At Pondurance, we recommend having 24/7 security monitoring in place to detect unwanted behavior and reduce the likelihood of an incident. Our MDR experts are available to help you build that plan or review your current plan. Learn more about MDR in our e-book: 5 Things To Consider When Choosing an MDR Vendor.



PONDURANCE

PONDURANCE

Copyright © 2021 Pondurance

About Pondurance

Pondurance delivers world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

Visit **www.pondurance.com** for more information.



Sources:
1. Security Today, The IoT Rundown for 2020: Stats, Risks, and Solutions, Jan 2020.
2. NIST, Cybersecurity Framework, 2021.

pondurance.com

500 N. MERIDIAN ST., STE. 500
INDIANAPOLIS, IN 46204