Homeland Security

Strategic Principles for Securing the Internet of Things

Overview

The growth of network-connected devices, systems and services comprising the Internet of Things (IoT)[1] creates immense opportunities and benefits for our society. Internet-connected devices enable seamless connections among people, networks, and physical services. Network-connected devices are becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. While the benefits of the IoT are undeniable, so too is the reality that security is not keeping up with the pace of innovation.

Prioritizing Security

As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

These non-binding strategic principles are designed to enhance security of the IoT across a range of design, manufacturing, and deployment activities, and include relevant suggested practices for implementation. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services and systems.

STRATEGIC PRINCIPLES FOR SECURING THE IOT:

- Incorporate Security at the Design Phase
- Promote Security Updates and Vulnerability Management
- Build on Recognized Security Practices
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

[1] In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

.

November 2016

Strategic Principles for Securing the IoT (version 1.0)

These principles are intended to equip stakeholders with tools to comprehensively account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for: IoT Developers, Manufacturers, Service Providers, and industrial and business-level consumers.

Incorporate Security at the Design Phase: Security should be evaluated as an integral component of any network-connected device. While there are notable exceptions, economic drivers motivate businesses to push devices to market with little regard for security.

Promote Security Updates and Vulnerability Management: Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies.

Build on Recognized Security Practices: Many tested practices used in traditional IT and network security can be used as a starting point for IoT security. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

Prioritize Security Measures According to Potential Impact: Risk models differ substantially across the IoT ecosystem, as do the consequences of security failures. Focusing on the potential consequences of disruption, breach, or malicious activity is critical for determining where in the IoT ecosystem particular security efforts should be directed.

Promote Transparency across IoT: Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Increased awareness can help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies.

Connect Carefully and Deliberately: IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.

The Department of Homeland Security

As a lead agency on cybersecurity, DHS places a strong emphasis on deterring and combatting cyber activities that threaten infrastructure, public safety, and ultimately the digital economy. The unprecedented size and scope of recent malicious cyber activities leveraging the IoT ecosystem has created urgency for the Department to prioritize security for the IoT. This effort is in line with DHS' mission to secure cyberspace, protect critical infrastructure, and ensure public safety. The Office for Cyber, Infrastructure, and Resilience Policy (CIR) is responsible for Department-wide policies and positions on issues related to cyber, technology, infrastructure, and resilience policy.

Contact Information

For more information go to www.dhs.gov/securingtheIoT

November 2016