NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

TRUSTED INTERNET OF THINGS (IOT) DEVICE NETWORK-LAYER ONBOARDING AND LIFECYCLE MANAGEMENT

The National Cybersecurity Center of Excellence (NCCoE) is addressing the challenges related to the implementation and use of trusted network-layer onboarding solutions and lifecycle management of IoT devices through collaborative efforts with industry and the information technology (IT) community, including vendors of cybersecurity solutions. This fact sheet provides an overview of the Trusted IoT Device Network-Layer Onboarding and Lifecycle Management, including background and challenge, goals, and potential benefits. If you would like to propose another architecture or know of products that might be applicable to the challenge, please contact us at iot-onboarding@nist.gov.

BACKGROUND

Provisioning network credentials to IoT devices in an untrusted manner leaves networks vulnerable to having unauthorized IoT devices connect to them. It also leaves IoT devices vulnerable to being taken over by unauthorized networks. Instead, trusted, scalable, and automatic mechanisms are needed to safely manage IoT devices throughout their lifecycles, beginning with secure ways to provision devices with their network credentials—a process known as trusted network-layer onboarding. Trusted network-layer onboarding, in combination with additional device security capabilities such as device attestation, application-layer onboarding, secure lifecycle management, and device intent enforcement, could improve the security of networks and IoT devices.

CHALLENGE

Network-layer onboarding is a particularly vulnerable point in an IoT device’s lifecycle because if it is not performed in a secure manner, both the device and the network are at risk. Its challenges include:

- Lack of a trusted way for an IoT device to verify a network’s identity when the IoT device is introduced to the network.
- Use of Wi-Fi over an open (unencrypted) network to provision network credentials.
- Use of a single, shared password across all devices.
- Lack of an automated and trusted mechanism for large organizations to provision and manage unique credentials to many IoT devices at one time.

GOALS

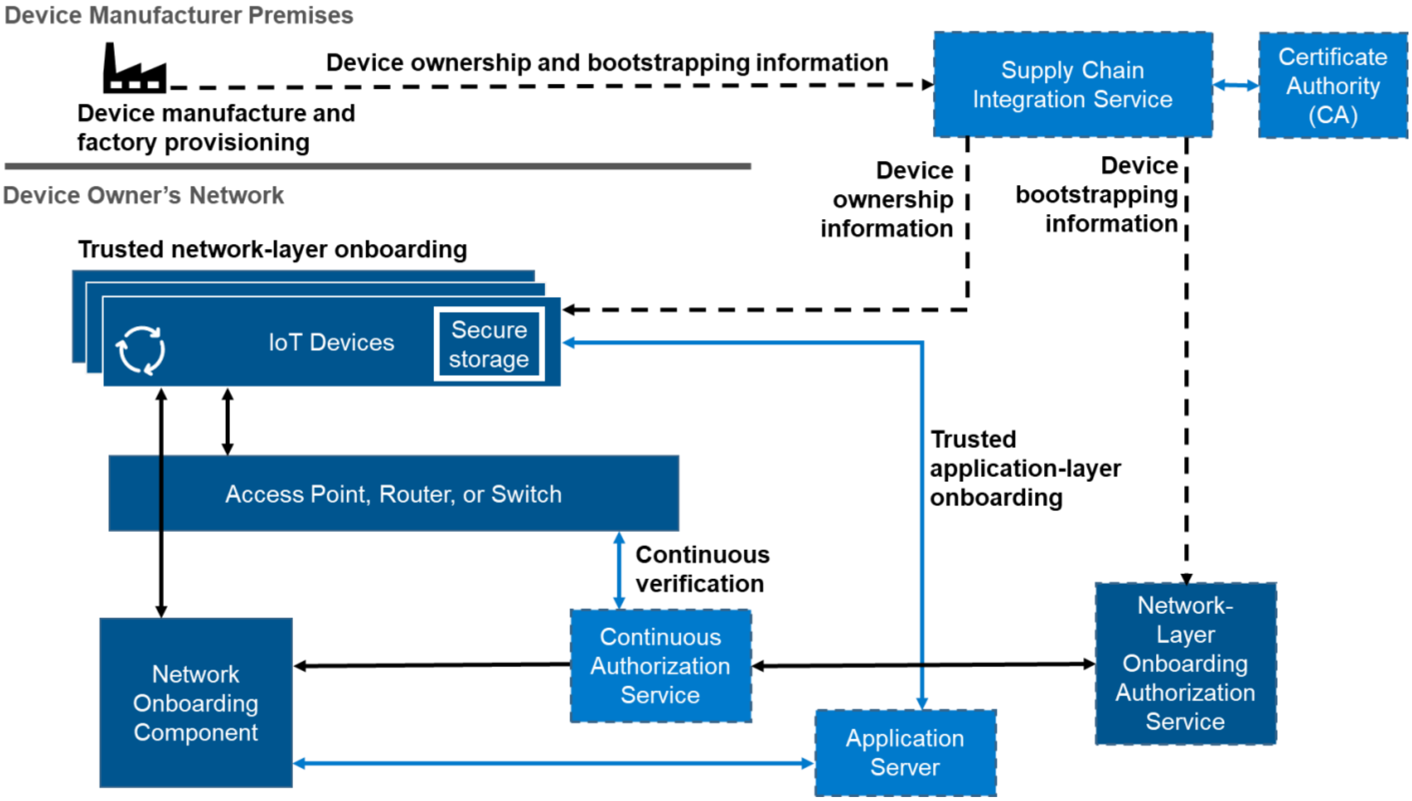
The goal of the project is to demonstrate how organizations can protect both their IoT devices and their networks. To achieve this, the NCCoE collaborated with product and service providers to produce example implementations of trusted network-layer onboarding and capabilities that improve device and network security throughout the IoT-device lifecycle.

BENEFITS

The potential benefits of securely providing IoT devices with their local network credentials include:

- Reduced costs associated with security breaches and incident response as a result of improved network-layer onboarding process.
- Scalable IoT deployments with confidence.
- Built customer trust through robust security measures.
- Improved network performance and reliability as a byproduct of trusted network-layer onboarding of IoT devices.

HIGH-LEVEL ARCHITECTURE FOR TRUSTED IOT ONBOARDING


Device Manufacturer Premises
Device ownership and bootstrapping information
Device manufacture and factory provisioning
Supply Chain Integration Service
Certificate Authority (CA)
Device Owner's Network
Device ownership information
Device bootstrapping information
Trusted network-layer onboarding
IoT Devices
Secure storage
Trusted application-layer onboarding
Access Point, Router, or Switch
Continuous verification
Network Onboarding Component
Continuous Authorization Service
Network-Layer Onboarding Authorization Service
Application Server

TECHNOLOGY COLLABORATORS

The technology vendors participating in this project submitted their capabilities in response to an open call in the Federal Register. Companies with relevant security capabilities were invited to sign a Cooperative Research and Development Agreement with the National Institute of Standards and Technology (NIST), allowing them to participate in a consortium to build this example solution.

Aruba, a Hewlett Packard Enterprise company
CableLabs
Cisco

Foundries.io
Kudelski IoT
NquiringMinds
NXP Semiconductors

Open Connectivity Foundation (OCF)
Sandelman Software Works

SEALSQ, a subsidiary of WISeKey
Silicon Labs

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or the NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

For more information about this project, visit:
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management

@NISTcyber

linkedin/showcase/nccoe