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

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) is collaborating with industry to address challenges related to the implementation and use of trusted network-layer onboarding solutions and lifecycle management of IoT devices.

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.

CHALLENGES

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 unique credentials to many IoT devices at one time.

GOAL

The goal of the project is to demonstrate how organizations can protect both their IoT devices and their networks. To achieve this, the NCCoE will collaborate 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

Trusted network-layer onboarding:

- Provides each device with unique network credentials.
- Provides the device and the network an opportunity to mutually authenticate.
- Is performed over an encrypted channel (to protect credential confidentiality).
- Does not provide anyone with access to the credentials.
- Can be performed repeatedly throughout the device lifecycle.

In turn, additional IoT device security may be achieved through integration with capabilities such as:

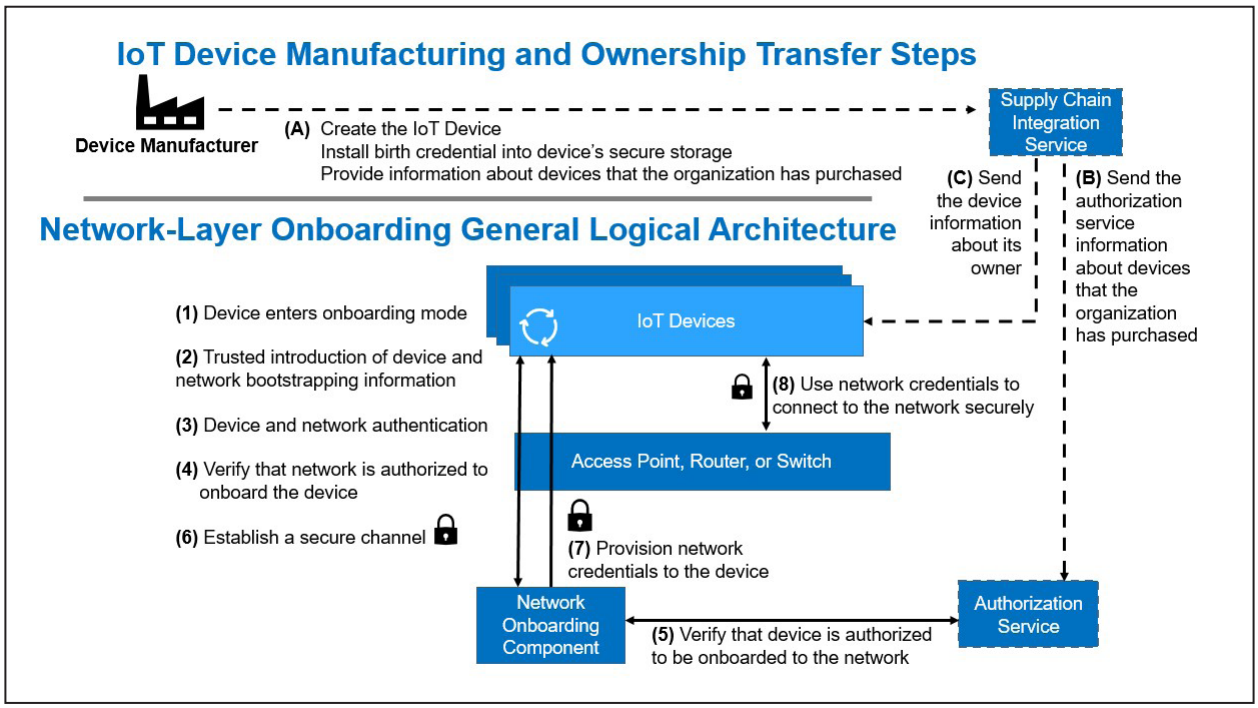
- Device attestation to verify device identity and determine device security state before it can be provisioned with credentials and granted access to the services on the network.
- Application-layer onboarding to connect the device with a trusted application service.
- Secure lifecycle management to ensure device posture through software and firmware updates.
- Device intent enforcement to allow only authorized communications to and from the device.

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights from businesses, the public, and technology vendors. If you have any questions about the project or would like to join the Community of Interest to receive the latest updates about the project, please email iot-onboarding@nist.gov.

HIGH-LEVEL ARCHITECTURE

Onboarding consists of two sets of inter-related activities: steps A-C, which are performed by the device manufacturer to make the device onboarding-ready and provide information about the device to the device's purchaser; and steps 1-8, which describes the automated process initiated by the device's purchaser to execute the trusted network-layer onboarding protocol that provisions the device with its network credentials.



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 NIST, allowing them to participate in a consortium to build this example solution. Project collaborators are listed below:

- Aruba, a Hewlett Packard Enterprise company
- CableLabs
- Cisco
- Foundries.io
- Kudelski IOT
- NquiringMinds
- NXP Semiconductors
- Open Connectivity Foundation
- Sandelman Software Works
- Silicon Labs
- WISeKey

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.

ABOUT THE NCCOE

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 ABOUT NCCOE

Visit the project page for the latest status of the project and to download the practice guide when it's released: https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management.

Visit the NCCoE website: https://www.nccoe.nist.gov

CONTACT US

nccoe@nist.gov | 301-975-0200

November 2022