NIST SPECIAL PUBLICATION 1800-36A

Trusted Internet of Things (IoT) Device Network-Layer Onboarding and Lifecycle Management:

Enhancing Internet Protocol-Based IoT Device and Network Security

Volume A:
Executive Summary

Michael Fagan
Jeffrey Marron
Paul Watrobski
Murugiah Souppaya
National Cybersecurity Center of Excellence
Information Technology Laboratory

Blaine Mulugeta
Susan Symington
The MITRE Corporation
McLean, Virginia

Dan Harkins
Aruba, a Hewlett Packard Enterprise company
San Jose, California

William Barker
Dakota Consulting
Silver Spring, Maryland

Michael Richardson
Sandelman Software Works
Ottawa, Ontario

May 2024

DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management

Executive Summary

Establishing trust between a network and an Internet of Things (IoT) device (as defined in [NIST Internal Report 8425](https://doi.org/10.6028/NIST.IR.8425)) prior to providing the device with the credentials it needs to join the network is crucial for mitigating the risk of potential attacks. There are two possibilities for attack. One happens when a device is convinced to join an unauthorized network, which would take control of the device. The other occurs when a network is infiltrated by a malicious device. Trust is achieved by attesting and verifying the identity and posture of the device and the network before providing the device with its network credentials—a process known as *network-layer onboarding*. In addition, scalable, automated mechanisms are needed to safely manage IoT devices throughout their lifecycles, such as safeguards that verify the security posture of a device before the device is permitted to execute certain operations. In this practice guide, the National Cybersecurity Center of Excellence (NCCoE) applies standards, best practices, and commercially available technology to demonstrate various mechanisms for trusted network-layer onboarding of IoT devices in Internet Protocol based environments. This guide shows how to provide network credentials to IoT devices in a trusted manner and maintain a secure device posture throughout the device lifecycle, thereby enhancing IoT security in alignment with the IoT Cybersecurity Improvement Act of 2020.

CHALLENGE

With 40 billion IoT devices expected to be connected worldwide by 2025, it is unrealistic to onboard or manage these devices by manually interacting with each device. In addition, providing local network credentials at the time of manufacture requires the manufacturer to customize network-layer onboarding on a build-to-order basis, which prevents the manufacturer from taking full advantage of the economies of scale that could result from building identical devices for its customers.

There is a need to have a scalable, automated mechanism to securely manage IoT devices throughout their lifecycles and, in particular, a trusted mechanism for providing IoT devices with their network credentials and access policy at the time of deployment on the network. It is easy for a network to falsely identify itself, yet many IoT devices onboard to networks without verifying the network's identity and ensuring that it is their intended target network. Also, many IoT devices lack user interfaces, making it cumbersome to manually input network credentials. Wi-Fi is sometimes used to provide credentials over an open (i.e., unencrypted) network, but this onboarding method risks credential disclosure. Most home networks use a single password shared among all devices, so access is controlled only by the device's possession of the password and does not consider a unique device identity or whether the device belongs on the network. This method also increases the risk of exposing credentials to unauthorized parties. Providing unique credentials to each device is more secure, but providing unique credentials manually would be resource-intensive and error-prone, would risk credential disclosure, and cannot be performed at scale.

Once a device is connected to the network, if it becomes compromised, it can pose a security risk to both the network and other connected devices. Not keeping such a device current with the most recent software and firmware updates may make it more susceptible to compromise. The device could also be attacked through receipt of malicious payloads. Once compromised, it may be used to attack other devices on the network.

OUTCOME

The outcome of this project is development of example trusted onboarding solutions, demonstration that they support various scenarios, and publication of the findings in this practice guide, a NIST Special Publication (SP) 1800 that is composed of multiple volumes targeting different audiences.

This practice guide can help IoT device users:

Understand how to onboard their IoT devices in a trusted manner to:

- **Ensure that their network is not put at risk** as new IoT devices are added to it
- **Safeguard their IoT devices** from being taken over by unauthorized networks
- **Provide IoT devices with unique credentials** for network access
- **Provide, renew, and replace device network credentials** in a secure manner
- **Support ongoing protection of IoT devices** throughout their lifecycles

This practice guide can help manufacturers and vendors of semiconductors, secure storage components, IoT devices, and network onboarding equipment:

Understand the desired security properties for supporting trusted network-layer onboarding and explore their options with respect to recommended practices for:

- **Providing unique credentials into secure storage on IoT devices at the time of manufacture to mitigate supply chain risks** (i.e., *device credentials*)
- **Installing onboarding software onto IoT devices**
- **Providing IoT device purchasers with information needed to onboard the IoT devices to their networks** (i.e., *device bootstrapping information*)
- **Integrating support for network-layer onboarding with additional security capabilities** to provide ongoing protection throughout the device lifecycle

SOLUTION

The NCCoE recommends the use of trusted network-layer onboarding to provide scalable, automated, trusted ways to provide IoT devices with unique network credentials and manage devices throughout their lifecycles to ensure that they remain secure. The NCCoE is collaborating with technology providers and other stakeholders to implement example trusted network-layer onboarding solutions for IoT devices that:

- provide each device with unique network credentials,
- enable the device and the network to mutually authenticate,
- send devices their credentials over an encrypted channel,
- do not provide any person with access to the credentials, and

- can be performed repeatedly throughout the device lifecycle.

The capabilities demonstrated include:

- trusted network-layer onboarding of IoT devices,
- repeated trusted network-layer onboarding of devices to the same or a different network,
- trusted application-layer onboarding (i.e., automatic establishment of an encrypted connection between an IoT device and a trusted application service after the IoT device has performed trusted network-layer onboarding and used its credentials to connect to the network), and
- software-based methods to provide device credentials in the factory and transfer device bootstrapping information from device manufacturer to device purchaser.

Future capabilities may include demonstrating the integration of trusted network-layer onboarding with zero trust-inspired [Note: See NIST SP 800-207] mechanisms such as ongoing device authorization, renewal of device network credentials, device attestation to ensure that only trusted IoT devices are permitted to be onboarded, device lifecycle management, and enforcement of device communications intent.

This demonstration follows an agile methodology of building implementations (i.e., *builds*) iteratively and incrementally, starting with network-layer onboarding and gradually integrating additional capabilities that improve device and network security throughout a managed device lifecycle. This includes factory builds that simulate activities performed to securely provide device credentials during the manufacturing process, and five network-layer onboarding builds that demonstrate the Wi-Fi Easy Connect, Bootstrapping Remote Secure Key Infrastructure (BRSKI), and Thread Commissioning protocols. These builds also demonstrate both streamlined and independent trusted application-layer onboarding approaches, along with policy-based continuous assurance and authorization. The example implementations use technologies and capabilities from our project collaborators (listed below).

Collaborators

- 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

While the NCCoE uses a suite of commercial products, services, and proof-of-concept technologies to address this challenge, this guide does not endorse these particular products, services, and technologies, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products and services that will best integrate with your existing tools, IT and IoT system infrastructure, and operations. Your organization can adopt these solutions or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, such as chief information security, product security, and technology officers, can use this part of the guide, *NIST SP 1800-36A: Executive Summary*, to understand the project's challenges and outcomes, as well as our solution approach.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-36B: Approach, Architecture, and Security Characteristics*. This part of the guide describes the architecture and different implementations. Also, *NIST SP 1800-36E: Risk and Compliance Management,* maps components of the trusted onboarding reference architecture to security characteristics in broadly applicable, well-known cybersecurity guidelines and practices.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-36C: How-To Guides*. It provides product installation, configuration, and integration instructions for building example implementations, allowing them to be replicated in whole or in part. They can also use *NIST SP 1800-36D*: *Functional Demonstrations,* which provides the use cases that have been defined to showcase trusted network-layer onboarding and lifecycle management security capabilities and the results of demonstrating these capabilities with each of the example implementations. These use cases may be helpful when developing requirements for systems being developed.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at https://www.nccoe.nist.gov/projects/building-blocks/iot-network-layer-onboarding. NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. As example implementations continue to be developed, you can adopt this solution for your own organization. If you do, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and recommended practices for transforming the processes associated with implementing this guide.

To provide comments, join the community of interest, or learn more by arranging a demonstration of these example implementations, contact the NCCoE at iot-onboarding@nist.gov.

COLLABORATORS

Collaborators participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). Those respondents with relevant capabilities or product components signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order 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 for the purpose.