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

December 2022

PRELIMINARY DRAFT

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

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Executive Summary

Providing devices with the credentials and policy needed to join a network is a process known as *network-layer onboarding*. Establishing trust between a network and an IoT device prior to such onboarding is crucial for mitigating the risk of potential attacks. There are two sides of this attack: one is where a device is convinced to join an unauthorized network, which would take control of the device. The other side is where 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 as part of the network-layer onboarding process. Additional safeguards, such as verifying the security posture of the device before other operations occur, can be performed throughout the device lifecycle. In this practice guide, the National Cybersecurity Center of Excellence (NCCoE) applies standards, recommended practices, and commercially available technology to demonstrate various mechanisms for trusted network-layer onboarding of IoT devices. We show how to provide network credentials to IoT devices in a trusted manner and maintain a secure posture throughout the device lifecycle.

CHALLENGE

With 40 billion IoT devices expected to be connected worldwide by 2025, it is unrealistic to onboard or manage these devices by visiting each device and performing a manual action. While it is possible for devices to be securely provided with their local network credentials at the time of manufacture, this 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.

The industry lacks scalable, automatic mechanisms to safely manage IoT devices throughout their lifecycles, and in particular it lacks a trusted mechanism for providing IoT devices with their network credentials and 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 the receipt of malicious payloads. Once compromised, it may be used to attack other devices on the network.

OUTCOME

The outcome of a project is to develop example solutions, demonstrate them to support various scenarios, and publish 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 time of manufacture** (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 has adopted the trusted network-layer onboarding approach to provide 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 initially 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 use cases we demonstrate include:

- trusted network-layer onboarding of IoT devices,
- repeated trusted network-layer onboarding of devices to the same or a different network,
- automatic establishment of an encrypted connection between an IoT device and a trusted application service (i.e., *trusted application-layer onboarding*) 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 use cases may include demonstrating the integration of trusted network-layer onboarding with zero trust-inspired capabilities such as ongoing device authorization, renewal of device network credentials, using device attestation to ensure that only trusted IoT devices are permitted to be onboarded, device lifecycle management, and enforcement of device communications intent.

We are following an agile methodology of building implementations iteratively and incrementally, starting with network-layer onboarding and gradually integrating additional capabilities that improve device and network security throughout a managed device lifecycle. There are five initial builds that demonstrate network-layer onboarding and one factory use case build intended to simulate activities performed by an IoT device manufacturer to provide devices with their credentials. The network-layer onboarding builds will demonstrate the Wi-Fi Easy Connect, Bootstrapping Remote Secure Key Infrastructure, and Thread Commissioning protocol approaches. Several application-layer onboarding approaches will also be implemented, along with policy-based continuous assurance and authorization.

The example implementations use technologies and capabilities from our project collaborators (listed below). The solutions will map to NIST Cybersecurity Framework security standards and guidelines, NIST Internal Report (NISTIR) 8259A capabilities, NISTIR 8228 considerations, and European Telecommunications Standards Institute (ETSI) European Standard (EN) 303 645 requirements.

Collaborators		
Aruba	Kudelski IoT	Sandelman Software Works
CableLabs	NquiringMinds	Silicon Labs
Cisco	NXP Semiconductors	WISeKey
Foundries.io	Open Connectivity Foundation	

While the NCCoE uses a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution 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 drivers, the challenges we address, our solution approach, and how the solution could benefit your organization.

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*, once it is available. It will describe what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-36C: How-To Guides*, once it is available. It will provide product installation, configuration, and integration instructions for building example implementations, allowing you to replicate all or parts of this project.

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. Work continues on implementing the example solutions and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized. The release cycle of the volumes will track closely with the completion of milestones achieved in the project.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. Once the example implementations are 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.