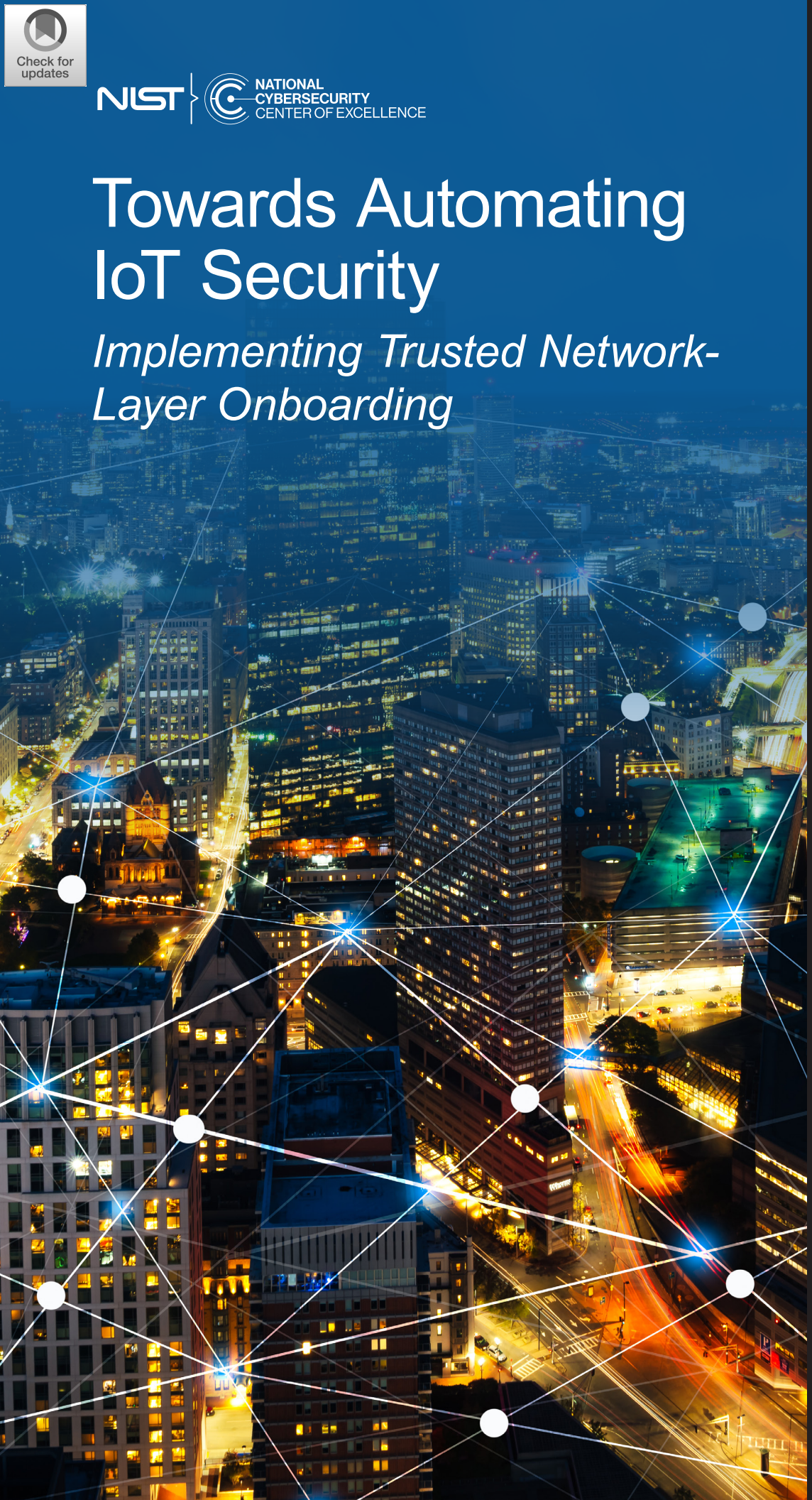
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Towards Automating IoT Security

Implementing Trusted Network-Layer Onboarding



NIST Cybersecurity White Paper

NIST CSWP 42 (DRAFT)

Michael Fagan
Jeffrey Marron
Murugiah Souppaya*
Paul Watrobski*
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity

Blaine Mulugeta
Susan Symington*
The MITRE Corporation

** Former employee; all work for this publication was done while at employer*

April 2025
Draft

DOI: https://doi.org/10.6028/NIST.CSWP.42.ipd

Abstract

This document provides an overview of trusted Internet of Things (IoT) device network-layer onboarding, a capability for securely providing IoT devices with their local network credentials in a manner that helps to ensure that the network is not put at risk as new IoT devices are connected to it— enhancing network security and management.

Audience

This paper is intended for individuals and organizations who use IoT devices to collect data from a variety of systems and locations in order to enable quick identification of potential issues and rapid response and management of them. For example, IoT devices could measure real-time data to detect component faults, measure toxins, or detect infrastructure breaches. Whether these IoT devices are used on complex operational networks or relatively simple home networks, the goal is to avoid exposing those networks and devices to additional threats.

Keywords

application-layer onboarding; bootstrapping; FIDO; Internet of Things (IoT); Manufacturer Usage Description (MUD); Matter; network-layer onboarding; onboarding; Wi-Fi Easy Connect;

Acknowledgments

We are grateful to the following individuals for their generous contributions to the trusted network-layer onboarding and lifecycle management project.

Aruba, a Hewlett Packard Enterprise company: Dan Harkins, Danny Jump

CableLabs: Andy Dolan, Kyle Haefner, Craig Pratt, Darshak Thakore

Cisco: Bart Brinkman, Eliot Lear, Peter Romness

Foundries.io: Tyler Baker, George Grey, David Griego

Kudelski IoT: Fabien Gremaud, Brecht Wyseur

NIST: Cherilyn Pascoe

NquiringMinds: Nicholas Allot, Toby Ealden, Alois Klink, John Manslow, Antony McCaigue, Alexandru Mereacre, Craig Rafter

NXP Semiconductors: Mihai Chelalau, Julien Delplancke, Anda-Alexandra Dorneanu, Todd Nuzum, Nicusor Penisoara, Laurentiu Tudor

Open Connectivity Foundation (OCF): Kyle Haefner

Sandelman Software Works: Michael Richardson

SEALSQ, a subsidiary of WISeKey: Steve Clark, Pedro Fuentes, Gweltas Radenac, Kalvin Yang

Silicon Labs: Mike Dow, Steve Egerter

The MITRE Corporation: Charlie Rearick, Joshua Klosterman, Faith Ryan

Overview

When an IoT device is deployed, it must be connected to a local network. To connect to that local network securely, the device must be provided with network credentials. If those network credentials are not unique to the device or are not provided in a secure manner, the network will be at increased risk of unauthorized or malicious devices connecting to it. Along the same lines, if an IoT device is not able to establish trust in the network it is joining it could be put at risk of onboarding to malicious networks.

What are the current IoT onboarding challenges?

With nearly 30 billion IoT devices forecasted to be connected worldwide by 2030 [1], there are several cybersecurity challenges that demand an automated, secure solution:

1. **Manual provisioning** of IoT devices is error-prone, time-consuming, and often insecure, especially at scale.
2. **Shared credentials** allow threats to propagate easily across devices.
3. **Limited user interfaces** on many IoT devices make manual credential input challenging or impossible.
4. **Open Wi-Fi networks** used for provisioning of network credentials increase the risk of eavesdropping and unauthorized access.
5. **Lack of device authentication** means that networks cannot verify if connecting devices truly belong.

How does trusted network-layer onboarding address the problem?

Trusted network-layer onboarding is an automated mechanism for securely provisioning network credentials to a device. Trusted network-layer onboarding and lifecycle management offers four key capabilities to address these challenges:

1. **Per-device network credentials**
   - Provides each device with unique network credentials.
   - Reduces attack surface and constrains potential damage.
   - Allows easy removal of individual compromised devices.
   - Prevents credential leakage between devices.
2. **Zero-touch onboarding**
   - Enables automated, scalable device onboarding.
   - Eliminates manual errors and security vulnerabilities.
   - Simplifies the process for both enterprise and consumer use cases.
3. **Configurable trust policies**
   - Allows customization of trust definitions based on specific use cases.
   - Enables flexible adaptation to various security requirements.
   - Encapsulates the onboarding method for different scenarios.

4. **Continuous assurance**
    - Implements zero-trust principles.
    - Enables ongoing policy-based device authorization.
    - Allows for immediate device removal if trust policies are breached.

These capabilities work together to:

- Enable mutual authentication between devices and networks.
- Securely transmit credentials over encrypted channels.
- Prevent unauthorized access to network credentials.
- Support repeated onboarding throughout a device's lifecycle.

By authenticating the identity of each device before providing the device with its network credentials, ensuring that each device receives unique credentials, and having those credentials encrypted while they are in-transit to the device, trusted network-layer onboarding helps ensure that the network will not be put at risk as new IoT devices are connected to it.

How can I use trusted network-layer onboarding?

The NCCoE Trusted IoT Device Network Layer Onboarding project recently implemented and demonstrated two different trusted network-layer onboarding protocols: Wi-Fi Easy Connect [2] and Bootstrapping Remote Secure Key Infrastructure (BRSKI) [3]. Wi-Fi Easy Connect leverages public key cryptography to ensure secure authentication and supports both Wi-Fi Protected Access 2 (WPA2) and WPA3 security standards, while BRSKI makes use of manufacturer-installed X.509 certificates and a registrar to establish mutual trust between the device and the network. The Wi-Fi Easy Connect protocol is particularly useful for devices with limited or no user interfaces, such as IoT devices in smart homes or enterprise settings, whereas BRSKI is designed for environments where devices need to be securely onboarded without user intervention, making it applicable to large-scale deployments. Irrespective of the use-case, Wi-Fi Easy Connect and BRSKI may be used to provide trusted network-layer onboarding in a manner that is more secure and easy to use. To leverage these protocols, IoT devices should be manufactured with support for the selected protocol, and target networks must be equipped with compatible onboarding components (e.g., Wi-Fi Easy Connect-enabled access point or a BRSKI-enabled registrar). It is the IoT device manufacturer's role to ensure that devices are designed to support one of the protocols and IoT device users' responsibility to select a protocol that aligns with their specific network requirements and the type of devices being onboarded. Individuals and organizations that want to take advantage of the enhanced security benefits offered by trusted network-layer onboarding may use either one of these protocols.

What else should I know about trusted network-layer onboarding?

Trusted network-layer onboarding is a continuous or recurring activity. Any given IoT device may need to be onboarded multiple times throughout its lifecycle, for example, to replace network credentials that need to be refreshed or to enable a device to be securely provisioned with credentials for a different network after being resold or repurposed. If a device supports Wi-Fi Easy Connect or BRSKI, these protocols may be used to provision the device with network credentials repeatedly, as needed throughout its lifetime.

Mutual Authentication

It is easy for a network to falsely identify itself, yet many IoT devices onboard to networks without first verifying the network's identity to ensure that it is their intended target network. By authenticating the network (in addition to authenticating the device), trusted network-layer onboarding helps protect the device from joining and being taken over by an unauthorized, imposter network.

Device Management Support

Once an IoT 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. While trusted network-layer onboarding is essential to the security of an IoT device and its network, it is important to also deploy additional security measures to securely update and manage IoT devices throughout the duration of their connection to the network to ensure that they remain secure.

Application-layer Onboarding

Trusted network-layer onboarding can provide a secure foundation for additional security measures used to protect the device and its network on an ongoing basis. For example, trusted network-layer onboarding can provide a foundation for trusted application-layer onboarding by providing the secure exchange of application-layer onboarding bootstrapping information between a device and an application server to which it needs to connect securely. Trusted network-layer onboarding can be immediately and automatically followed by trusted application-layer onboarding, ensuring that a device is securely provisioned not only with its network credentials, but also with application-layer credentials. The device's application server may then be used to securely download the most recent version of the device's application to it, as well as to provide ongoing lifecycle management for the device, updating and patching its software as needed to maintain a secure posture on an ongoing basis. The example implementations built as part of the NCCoE Trusted IoT Device Network-Layer Onboarding project demonstrated IoT devices automatically performing several different types of trusted application-layer onboarding following successful trusted network-layer onboarding and network connection.

Beyond the examples of trusted network-layer onboarding integrated with application-layer onboarding demonstrated in this project, like Wi-Fi Easy Connect and Open Connectivity Foundation's (OCF) IoTivity, there are additional methods of demonstrating this capability. An example of this is the integration of the Wireless Broadband Alliance's (WBA) OpenRoaming framework with the FIDO Device Onboard (FDO) protocol, developed by the FIDO Alliance, which uses asymmetric public key cryptography to provide a secure method for onboarding IoT devices to any device application-layer management system [4]. Another application-layer

protocol in this space is Matter, developed by the Connectivity Standards Alliance (CSA). It incorporates built-in components for secure device application-layer onboarding, utilizing device identity and certificate-based authentication. This application-layer onboarding protocol supports various network transports, including Wi-Fi, Thread, and Ethernet, making it a versatile option for a variety of IoT device network-layer onboarding protocols [5].

Additional Security Capabilities

Trusted network-layer onboarding can also provide a secure foundation for additional security mechanisms, such as device communications intent enforcement (e.g., Manufacturer's Usage Description—MUD [6]). MUD provides a standard way to specify the network communications that an IoT device requires to perform its intended functions. For example, the Wi-Fi Easy Connect protocol is specifically designed with the option of securely conveying the MUD file URL from the device to the network. If the network is equipped to support MUD, the Wi-Fi Easy Connect trusted network-layer onboarding process can securely provide the network with the device intent information that it needs to ensure that only traffic that is required for the device to fulfill its designated purpose will be permitted to be sent from and received by the device.

One of the example implementations built as part of the NCCoE project demonstrated several zero trust-inspired capabilities for performing continuous device authorization after the completion of trusted network-layer onboarding. This build performed a set of ongoing policy-based assurance checks and removed the device from the network if, for example, the vulnerability score for the device's software bill of materials was determined to be below a set threshold, the device attempted to contact an IP address that was on a deny list, or the manufacturer of the device was no longer trusted.

For background information on the NCCoE Trusted IoT Device Network-Layer Onboarding project, including the functionality supported by five example trusted IoT device onboarding implementations prototyped within the demonstration lab environment, see NIST SP 1800-36, Volume B, Trusted IoT Device Network-Layer Onboarding and Lifecycle Management: Approach, Architecture, and Security Characteristics.

References

[1] Vailshery L (2024) Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033. Statista. Available at https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] Wi-Fi Alliance (2020) Wi-Fi Easy Connect™ Specification Version 3.0. Available at https://www.wi-fi.org/system/files/Wi-Fi_Easy_Connect_Specification_v3.0.pdf

[3] Pritikin M, Richardson M, Eckert T, Behringer M, Watsen K (2021) Bootstrapping Remote Secure Key Infrastructure (BRSKI). (RFC Editor), Request for Comments (RFC) RFC 8995. https://doi.org/10.17487/RFC8995

[4] Wireless Broadband Alliance (2025) Openroaming for IoT — FIDO Device Onboard Framework. Available at: https://wballiance.com/openroaming-for-iot-fido-device-onboard-framework/

[5] Connectivity Standards Alliance (2025). Matter: The Foundation for Connected Things. Available at: https://csa-iot.org/all-solutions/matter/

[6] Lear E, Droms R, Romascanu D (2019) Manufacturer Usage Description Specification. (RFC Editor), Request for Comments (RFC) RFC 8520. https://doi.org/10.17487/RFC8520

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 NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements

NIST Technical Series Publication Identifier Syntax

Author ORCID iDs

Michael Fagan: 0000-0002-1861-2609, Jeffrey Marron: 0000-0002-7871-683X,
Karen Scarfone: 0000-0001-6334-9486 , Murugiah Souppaya 0000-0002-8055-8527,
Paul Watrobski 0000-0002-6449-3030

How to Cite this NIST Technical Series Publication:

Fagan M, Marron J, Souppaya M, Watrobski P, Scarfone K, Mulugeta B, Symington S (2025) Towards Automating IoT Security: Implementing Trusted Network-Layer Onboarding. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 42 ipd. https://doi.org/10.6028/NIST.CSWP.42.ipd

Public Comment Period

April 14th 2025 – May 29th 2025

Submit Comments

iot-onboarding@nist.gov or submit the web form at
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000)
Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at
https://www.nccoe.nist.gov/projects/trusted-iot-device-network-layer-onboarding-and-lifecycle-management,
including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE