Trusted IoT Network-Layer Onboarding and Lifecycle Management –
Enhancing Internet Protocol-Based IoT Device and Network Security

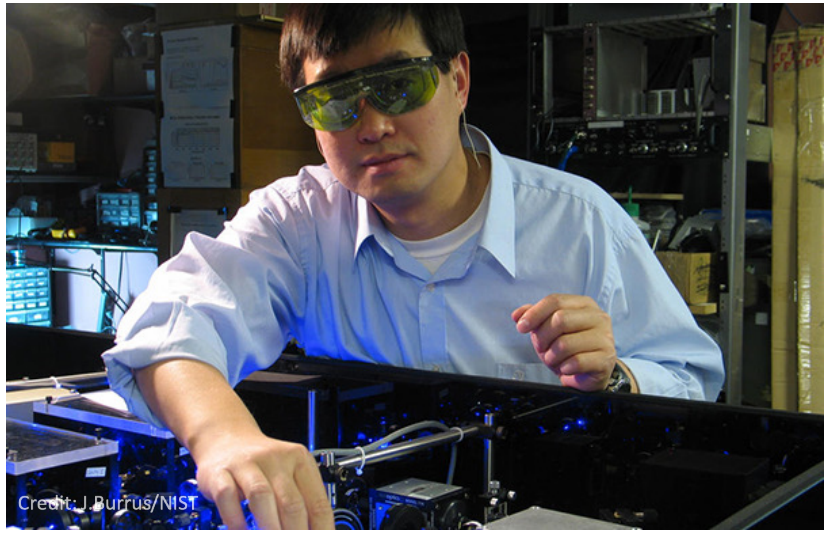
June 2021

NCCoE
National Cybersecurity Center of Excellence

National Institute of Standards and Technology

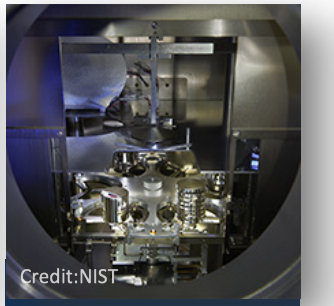
NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life



NIST Laboratory Programs

Material Measurement Laboratory

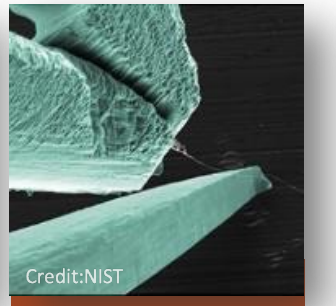


Physical Measurement Laboratory

Engineering Laboratory

Information Technology Laboratory

Communication Technology Laboratory



Center for Nanoscale Science and Technology

NIST Center for Neutron Research

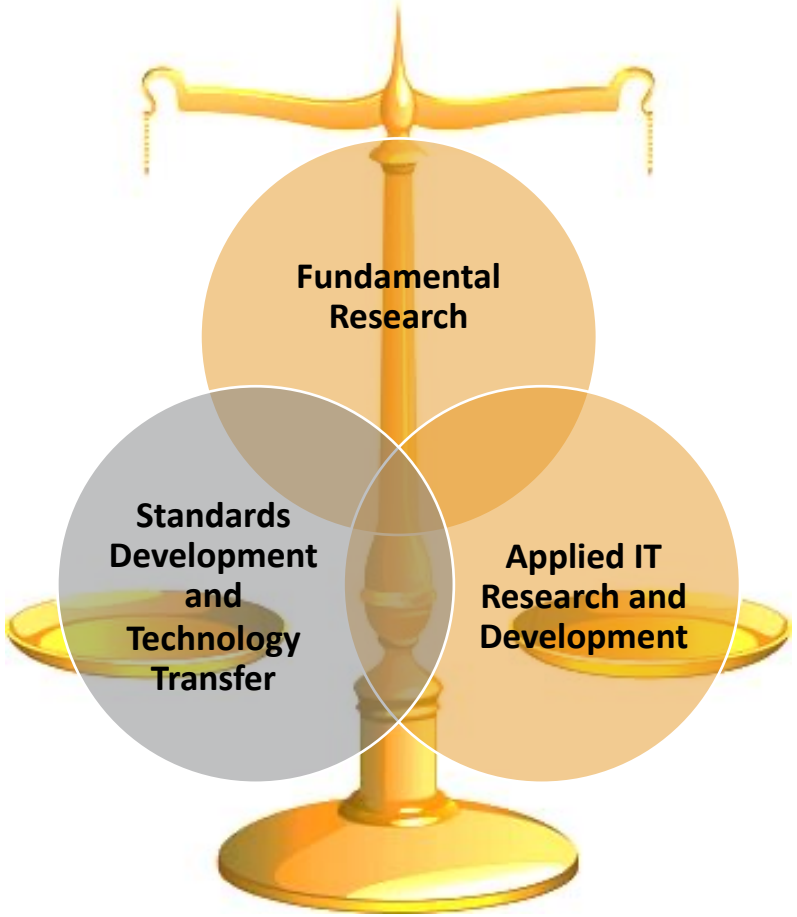
Information Technology Laboratory – itl.nist.gov

Cultivating Trust in IT and Metrology

Cybersecurity Program

Standards and Guidelines Development – csrc.nist.gov

- Cryptographic Development – AES, SHA-3, PQC, etc.
- Cryptographic Validation – FIPS 140-3
- Risk Management Framework – Cybersecurity Framework, FISMA, SP 800-53, SP 800-171, etc.
- Technology Guidelines – Virtualization, Containers, Security Automation, etc.
- Framework for cybersecurity, privacy, workforce, and secure software development
- Identity Management



National Cybersecurity Center of Excellence (NCCoE) – nccoe.nist.gov

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

- DEFINE
- ASSEMBLE
- BUILD
- ADVOCATE

Collaboration with Industry, Federal/State/Local Governments, and Academia

Introduction to NCCoE

NCCoE Mission

NCCoE Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

OUTCOME:
Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

BUILD

OUTCOME:
Build a practical, usable, repeatable implementation to address the cybersecurity challenge

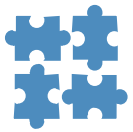
ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the practice guide

NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards



Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable

Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent

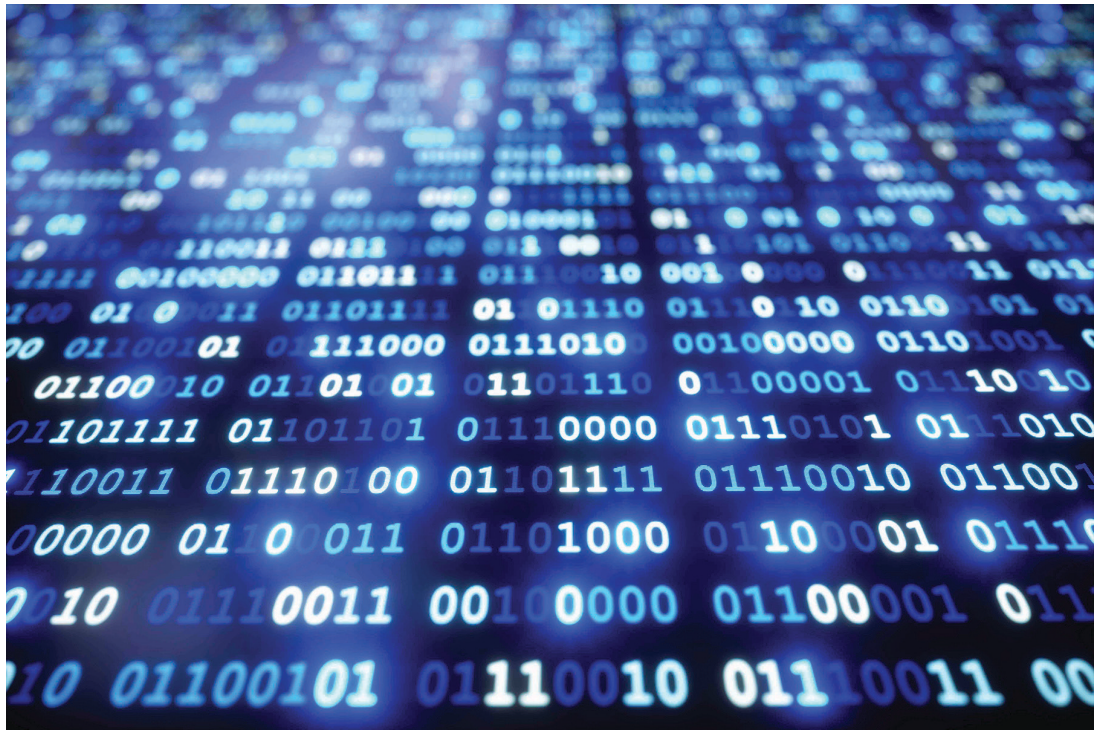
Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

SP 1800 Series: Cybersecurity Practice Guides

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

- Volume A: Executive Summary
  - High-level overview of the project, including summaries of the challenge, solution, and benefits
- Volume B: Approach, Architecture, and Security Characteristics
  - Deep dive into challenge and solution, including approach, architecture, and security mapping to the Cybersecurity Framework and other relevant standards
- Volume C: How-To Guide
  - Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

Sector-Based Projects



- Commerce/Retail (SP 1800-17)
- Energy (SP 1800-2 & SP 1800-7)
- Financial Services (SP 1800-5 & SP 1800-9 & SP 1800-18)
- Healthcare (SP 1800-1 & SP 1800-8)
- Hospitality
- Manufacturing
- Public Safety/First Responder (SP 1800-13)
- Transportation

Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS (SP 1800-15)
- Mobile Device Security (SP 1800-4 & SP 1800-21)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (SP 1800-19)

Trusted IoT Network-Layer Onboarding Building Block

Trusted IoT Network-Layer Onboarding: Objective

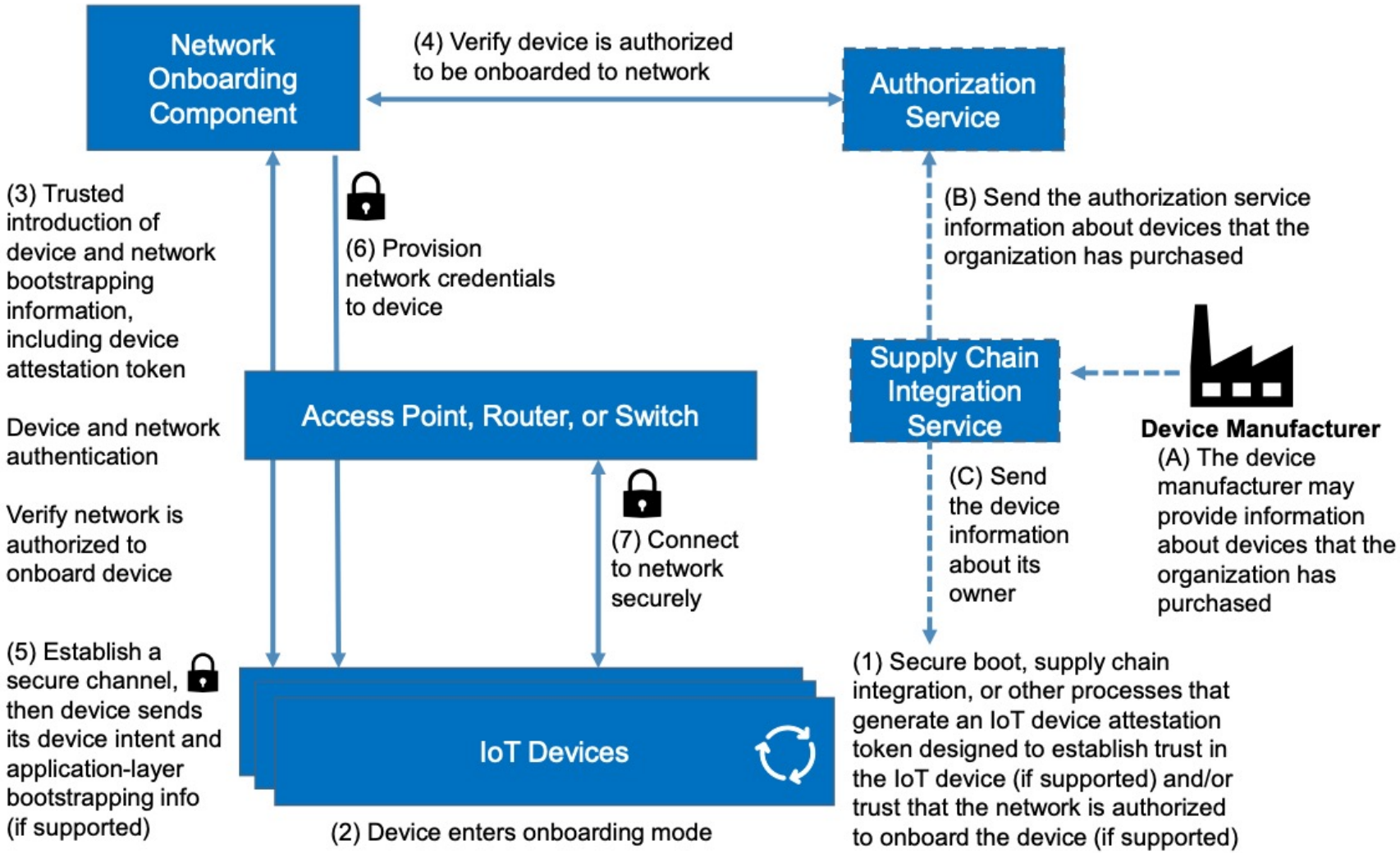
- Number of IoT devices is exploding
  - Estimated 40 billion IoT devices by 2025
  - The growing number of IoT devices is leading to an expanding attack surface
  - We need scalable mechanisms to safely manage IoT devices throughout their lifecycles
    - Network credential provisioning
    - Device intent
    - Device attestation
    - Application-layer onboarding
    - Additional zero-trust-inspired mechanisms

Sources: Statista: • Number of connected devices worldwide 2030 | Statista (38.6 billion)
International Data Corporation (IDC): 41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025 - Help Net Security (41.6 billion)

Trusted IoT Network-Layer Onboarding: Scope

- **Trusted Network-layer Onboarding** - provides assurance that a network is not put at risk as new IoT devices are added to it
  - Device is provisioned with unique credentials
  - Device and network have the opportunity to authenticate each other
  - Provisioning occurs over an encrypted channel
  - No humans are given access to the credentials
  - Can be performed repeatedly throughout the device lifecycle

High Level Architecture



Scenarios

Current Scenarios

- **Scenario 1: Trusted network-layer onboarding**
  - identities of the device and the network are authenticated
  - network onboarding component provisions unique network credentials to the device over a secure channel
- **Scenario 2: Validation of device authenticity and integrity**
  - performing attestation, supply chain management (e.g., hardware, firmware, and software component inventory), configuration monitoring, or other asset-management-related operations on an IoT device to validate its authenticity and integrity.
  - may be performed as part of a trusted boot process or at some other point before permitting the device to be onboarded to the network
- **Scenario 3: Trusted application-layer onboarding**
  - trusted application-layer onboarding that is performed automatically on an IoT device after it connects to a network
- **Scenario 4: Re-onboarding a wiped device**
  - re-onboarding an IoT device to a network after wiping it clean of any stored data so that it can be re-credentialed and re-used.
- **Scenario 5: Onboarding with device intent enforcement**
  - onboarding an IoT device to a network, augmented with a mechanism for device intent enforcement (for example, Manufacturer Usage Description [MUD])

Status

Current Status

- **Host virtual workshop**
  - October 2020
- **Publish draft project description**
  - March 2021
- **Publish final project description**
  - May 2021
- **Initiate the Federal Register Notice (FRN)**
  - May 2021
- **Publish FRN and solicit letter of interest (LOI)**
  - July 2021
- **Establish cooperative research and development agreement (CRADA)**
  - August 2021
- **Project kickoff meeting**
  - September 2021
- **Design, build, demonstrate, document, and outreach**
  - September 2021 to September 2022

Wrap Up: We Value Your Feedback

- Do you:
  - Have additional comments/feedback regarding our project?
  - Have an idea that you think the NCCoE should pursue?

- Please engage with us: IoT-Onboarding@nist.gov

https://www.nccoe.nist.gov

301-975-0200

IoT-Onboarding@nist.gov