CYBERSEC 2024
臺灣資安大會
5/14 Tue – 5/16 Thu
臺北南港展覽二館
Generative Future

AIoT & Hardware Security Summit

當資安已經不是選項-為物聯網資安認證做好準備

Joe Wang

Business Development

Joe.wang@keysight.com

Who is Keysight

Solutions Designed for Key Markets

COMMERCIAL COMMUNICATIONS

AEROSPACE AND DEFENSE

AUTOMOTIVE AND ENERGY

SEMICONDUCTORS AND MANUFACTURING

GENERAL ELECTRONICS

[1] As of March 2020

KEYSIGHT

We Offer End-to-End Solutions Across Workflows and Markets

MARKETS

WORKFLOW

Design → Emulate → Prototype → Test → Manufacture → Optimize

Acquisitions to Enhance Capabilities and Expertise

5G, Networking, and Computing Solutions

Anite

ixia

MICRAM

prisma telecom testing

SCALABLE NETWORK TECHNOLOGIES

SANJOLE

Quantum Solutions

Signadyne

quantum benchmark

Labber QUANTUM

Software for Electronic Design and Test

eggplant

Quamotion Make your app shine

cliosoft

Automotive and Energy Solutions

scienlab electronic systems

nordsys NORDDEUTSCHE SYSTEMTECHNIK

verisco Verified Smart Communication

Services

Electroservices

Liberty Calibration

THALES Australia Calibration Services

PSNA

Supplier

Swiss-Micron

Validate Cybersecurity of Connected Devices, Critical Deployments, and Vehicles

Emulate cyberattacks with unparalleled fidelity

- Test networks, vehicles, and devices against complex, multistage attacks
- Comply with cybersecurity standards and regulations, including U.S. Cyber Trust Mark and UN R155 (EU)

Test your products and networks against the latest threats

- Ensure operational safety for critical deployments in industrial, automotive, IoT, healthcare, and government sectors
- Fine-tune security detection and mitigation tools by testing against real-world cyber threat simulations

IoT Security

Keysight Is a World Leader In Test and Measurement

Helping To Shape The World of IoT

Member of multiple industry standard bodies

- Technological Advisory Council (TAC) for the Federal Communications Commission (FCC)
- O-RAN Alliance, 5G-Advanced and early 6G research
- Industry consortia (IOWN, NextG Alliance, QED-C)

Cyber Security Trust Mark

- White House announced Cyber Trust Mark for consumer IoT devices that pass cybersecurity tests and are transparent about data usage
- Keysight was one of a few select vendors and the only testing solution provider invited to participate

U.S. Cybersecurity Labeling Program for Smart Devices

U.S. CYBER TRUST MARK

Image Credits: FCC

Security Is No Longer Optional

Growth in compliance and standards for consumer and enterprise IoT devices

01 Broad IoT Device Security Standards

ETSI EN 303 645

ISO/IEC 27402

NIST IR 8425

IEEE 1547.3-2023

ISA/IEC 62443

02 National Consumer IoT Labelling

US Cyber Trust Mark

Singapore CLS

The UK Product Security and Telecommunications Infrastructure

03 International Technology Standards

ORAN Alliance

Open Web Application Security Project (OWASP)

CTIA for cellular IoT

04 Sector Standards & Specifications

Transport | TSA | Pipeline Operators

Defense | CMMCv2.0 | Defense Contractors

Energy | UL 2941 | Distributed Energy Resources (DER)

Automotive | UN ECE WP.29 Vehicles

Why Test ?

How to manage the growing risk

IoT devices are at risk

- 87% increase in IoT malware attacks in 2022[1].
- 57% of IoT devices are at risk of medium or high-severity attacks[2].
- 98% of traffic sent by IoT devices is unencrypted, exposing huge quantities of personal and confidential data to potential attackers[2].

Organizations lack skills and visibility

- 42% say they lack the ability to detect vulnerabilities on IoT and OT devices[3].
- 64% have low or average confidence that IoT devices are patched and up to date[3].

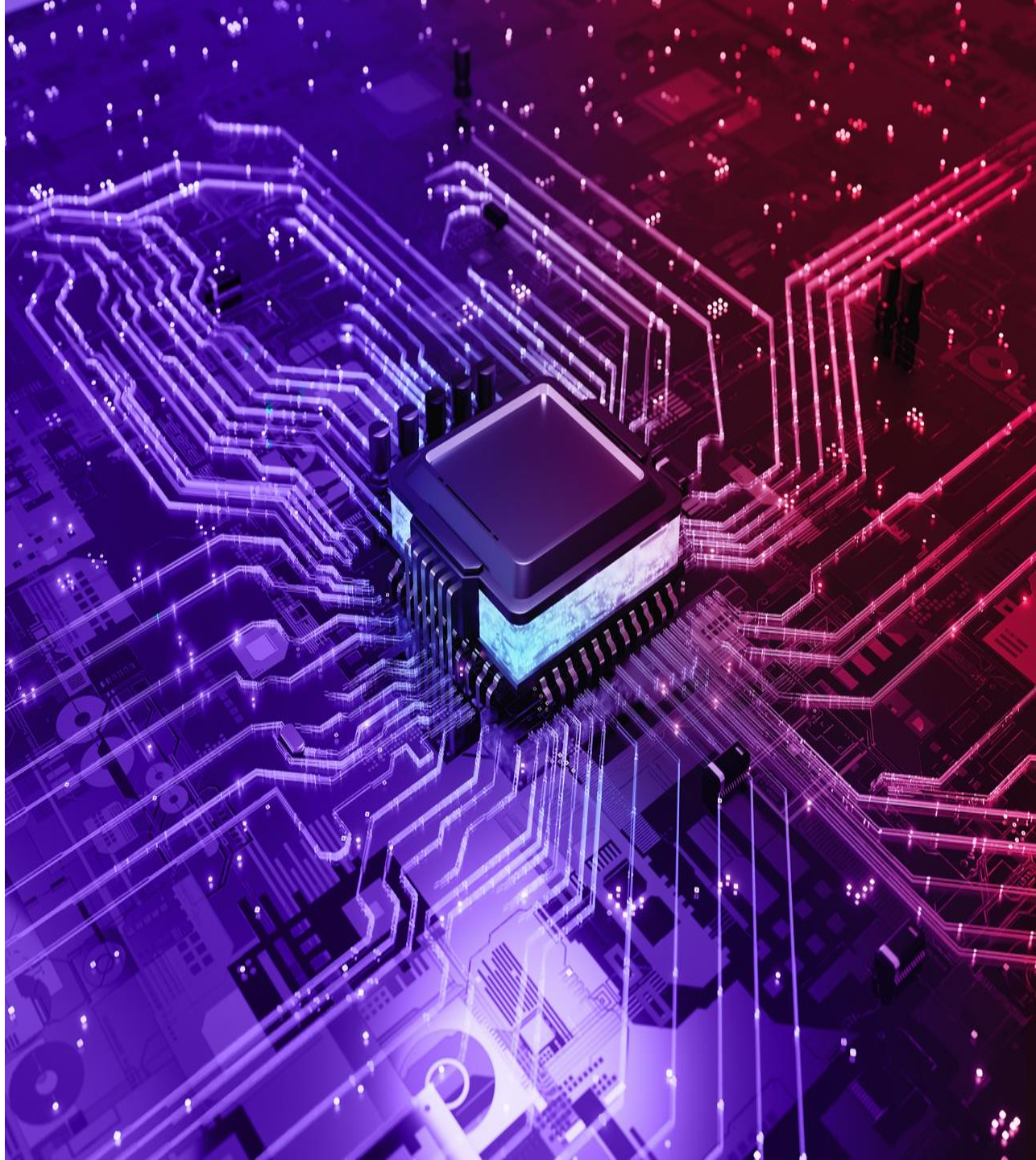
The Importance of Firmware Security

Detecting Vulnerability on IoT Device Firmware

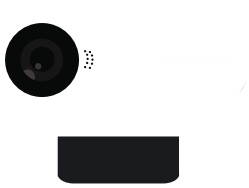
Firmware Security Is Essential

- IoT devices make up 30% of all network-connected endpoints, introducing vulnerabilities and novel attacks that make many companies as primary targets for cybercriminals[1].
- Firmware analysis has never been an easy job due to the diversity and closed nature of the environment[1].
- The absence of necessary interfaces and constrained hardware resources, makes firmware often invisible to network-based security tools.
- This invisibility makes firmware vulnerabilities harder to detect and, consequently, more challenging to address.

Source: IEEE/CAA Journal of Automatica Sinica (2023)

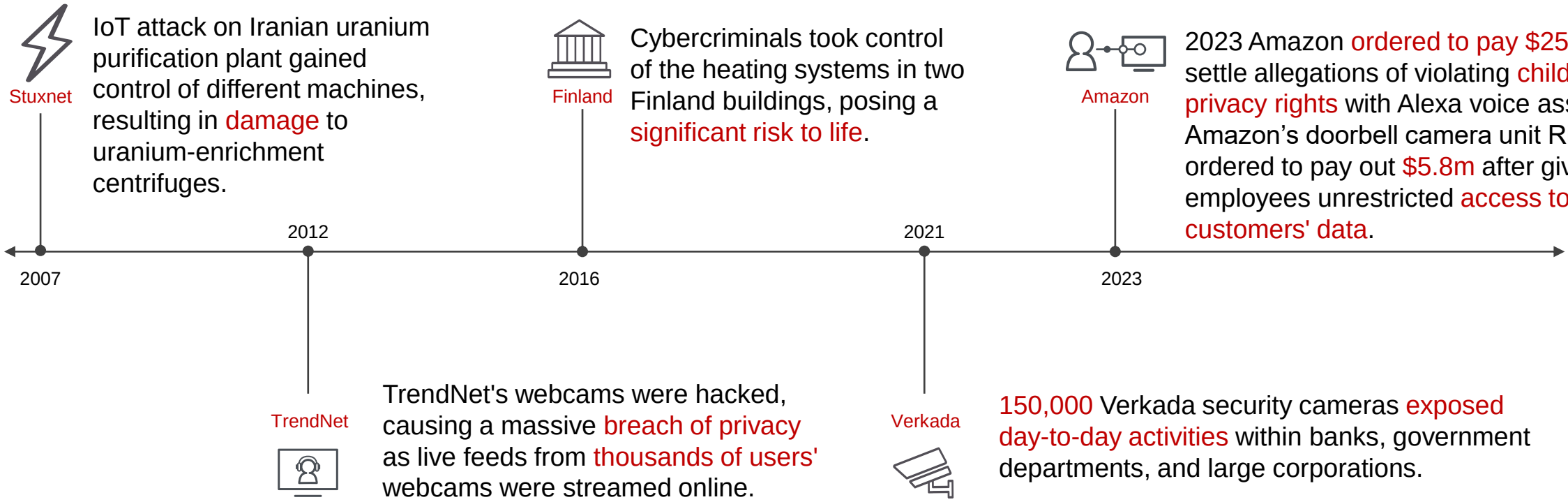


IoT Device Vulnerabilities

Examples of 5 recent IoT security gaps	
	ICSA-22-172-03 Can allow an attacker to execute malicious code on the device.
	ICSA-20-063-01 Can grant access control to a thief by means of remote execution.
	CVE-2021-39238 Enables remote code execution, can spread across network.
	CVE-2021-28372 Allows hackers to watch and listen to live feeds.
	CVE-2021-33883 Allows altered doses of medication to be delivered to patients without any checks.

Insufficient Testing Will Cost You Time, Money and Reputational Damage

Timeline of example IoT attacks



- When you discover vulnerabilities, you must scramble to address flaws and rush updates
- You risk brand damage, expensive recalls, compliance risk and potential fines
- Result of inadequate full-stack testing

Insufficient Supply Chain Testing Puts You at Risk

Off-the-shelf communication chipsets may not be fully tested or have latest firmware

- Vulnerabilities often lurk in third-party Systems on Chip (SoC).
- These issues are notoriously difficult for device manufacturers to find, and you usually can't fix them directly.
- Comprehensive IoT device testing may appear difficult and costly, and you need the right skills.

KEYSIGHT

FDA U.S. FOOD & DRUG ADMINISTRATION

SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication

The U.S. Food and Drug Administration (FDA) is informing patients, health care providers, and manufacturers about the SweynTooth family of cybersecurity vulnerabilities, which may introduce risks for certain medical devices. The FDA is not aware of any confirmed adverse events related to these vulnerabilities. Software to exploit these vulnerabilities in certain situations is already publicly available.

The potential impacts of the SweynTooth vulnerabilities fall into three categories. An unauthorized user can wirelessly exploit these vulnerabilities to:

- **Crash** the device. The device may stop communicating or stop working.
- **Deadlock** the device. The device may freeze and stop working correctly.
- **Bypass security** to access device functions normally available only to an authorized user.

The FDA is currently aware of several system-on-a-chip (SoC) manufacturers that are affected by these vulnerabilities:

- Texas Instruments
- NXP
- Cypress
- Dialog Semiconductors
- Microchip
- STMicroelectronics
- Telink Semiconductor

What is the Cyber Trust Mark?

The US Cyber Trust Mark labeling program establishes crucial standards around data privacy and cybersecurity for IoT devices. Building on the pioneering work of the National Institute of Standards and Technology (NIST) and the Federal Communications Commission (FCC), the program aims to help consumers make more informed choices about the connected devices they purchase, including those that monitor their households and health.

The full specifics of the Cyber Trust Mark won't be finalized until late 2024. However, the final standard will likely be based on existing IoT security standards, such as ETSI EN 303 645 and ANSI / CTA-2088-A. Keysight is working with industry leaders and the government to ensure that the standard is rigorous and testable for automated certification. Key areas for certification will include strong and unique default passwords, data security, secure update mechanisms, and incident detection pathways. In addition to passing a battery of security tests, the Cyber Trust Mark program may also require manufacturers to disclose the data their device collects and how it will be used.

Based on initial guidance from the FCC, external lab testing will be a requirement for Cyber Trust Mark certification. This helps maintain a high quality of independent testing while incentivizing manufacturers to pass certification on the first try. Otherwise, they'll incur additional costs and time-to-market delays.

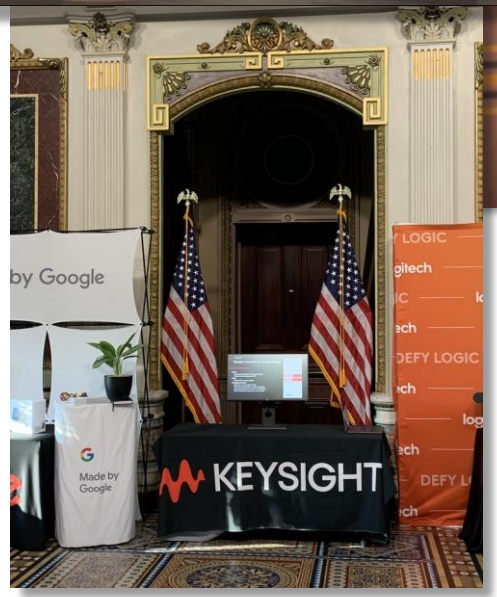
Keysight Participates in White House IOT Cybersecurity Announcement

Enabling a more secure nation via cybersecurity improvements

- The White House announced on Tuesday, July 18th, a new voluntary Cyber Trust Mark for consumer IOT devices which pass cybersecurity tests and are transparent about data usage
- Keysight was one of a select set of vendors – and the only testing solution provider – invited to participate
- Keysight is key to the program's success by making automated certification testing available to all IOT device manufacturers via its IOT Security Assessment software

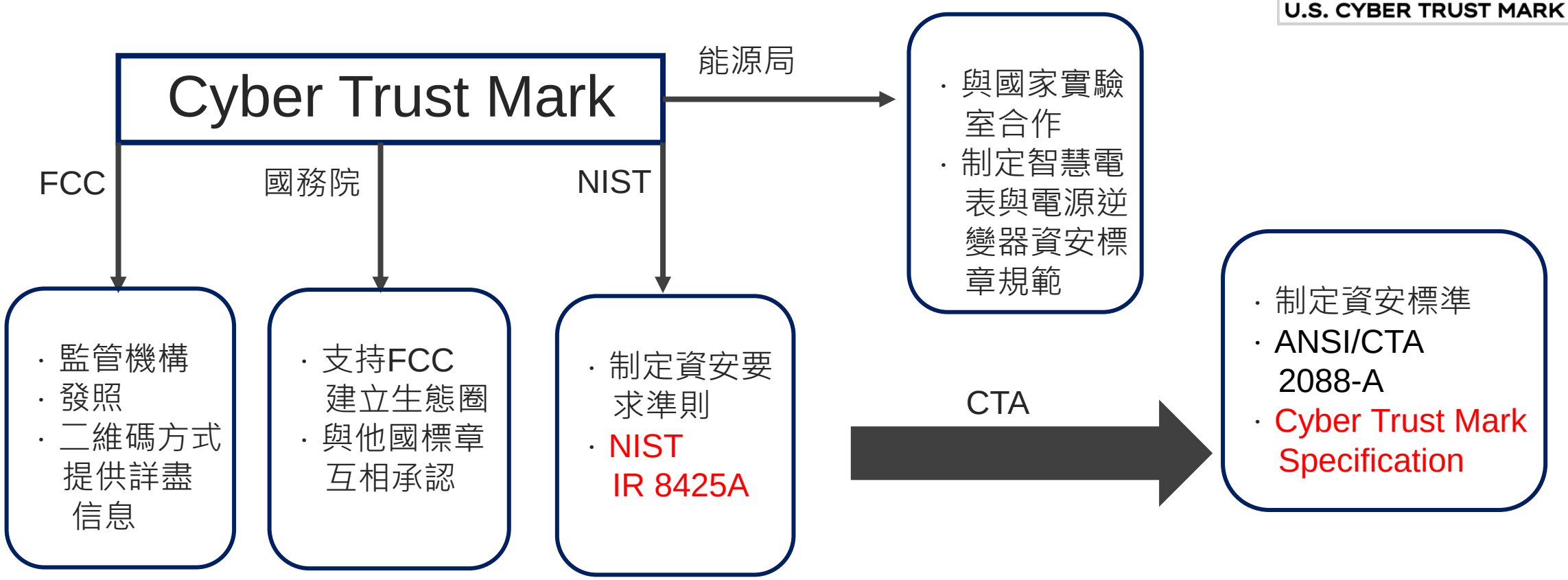
Deputy National Security Advisor Anne Neuberger and industry leaders from Keysight, Google, Amazon, UL and others at the White House

Ram Periakaruppan, Keysight VP and GM, addressing Keysight's critical role in the ecosystem



Keysight's IOT Security demonstration highlighting automated cybersecurity testing

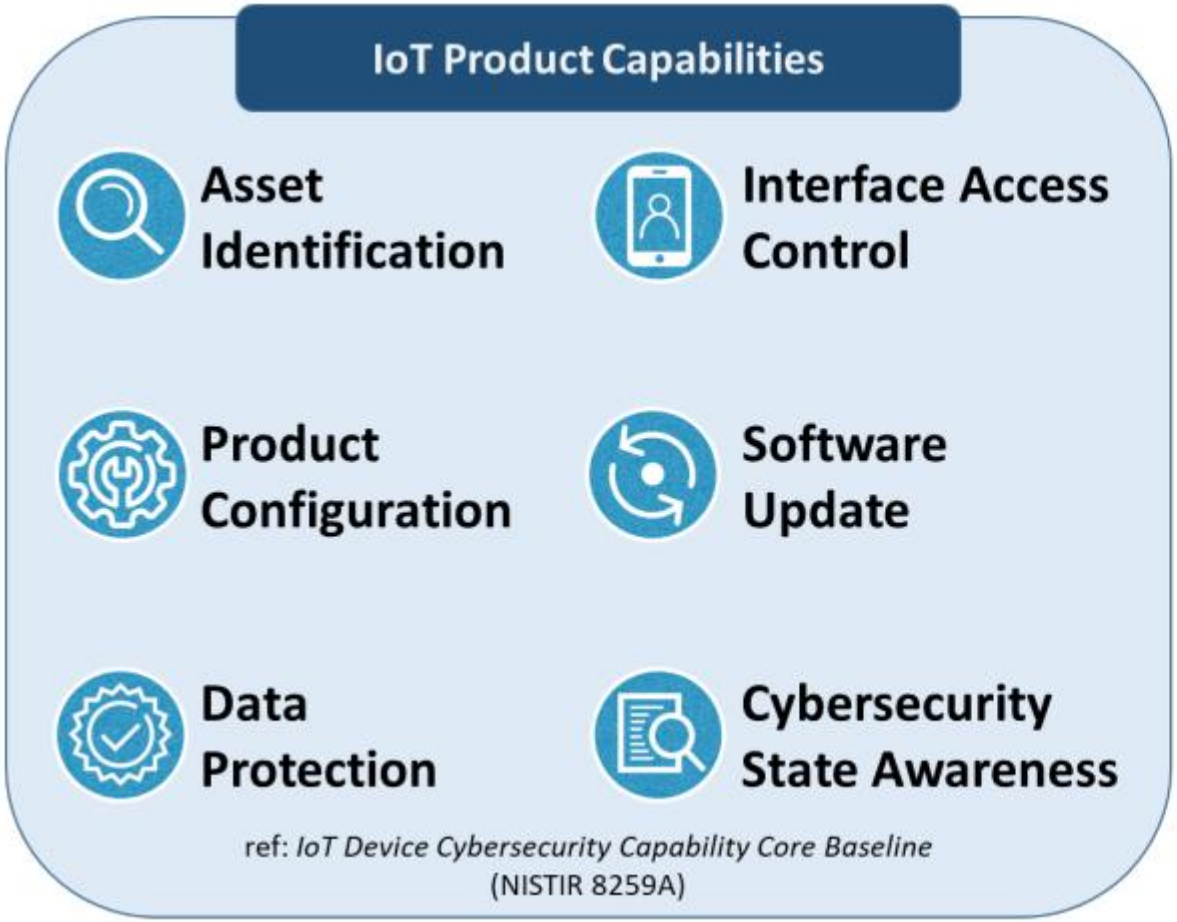
White House Announcement

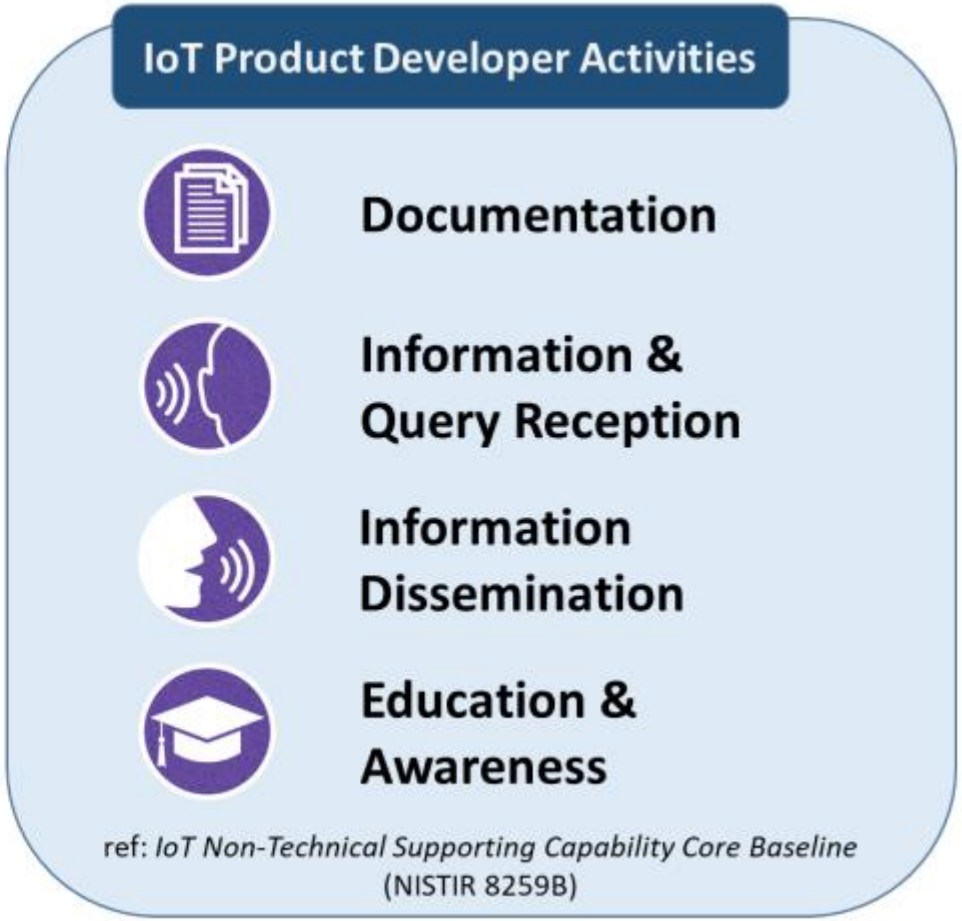


Source: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/18/biden-harris-administration-announces-cybersecurity-labeling-program-for-smart-devices-to-protect-american-consumers/

NIST IR 8425

Profile of the IoT Core Baseline for Consumer IoT Products

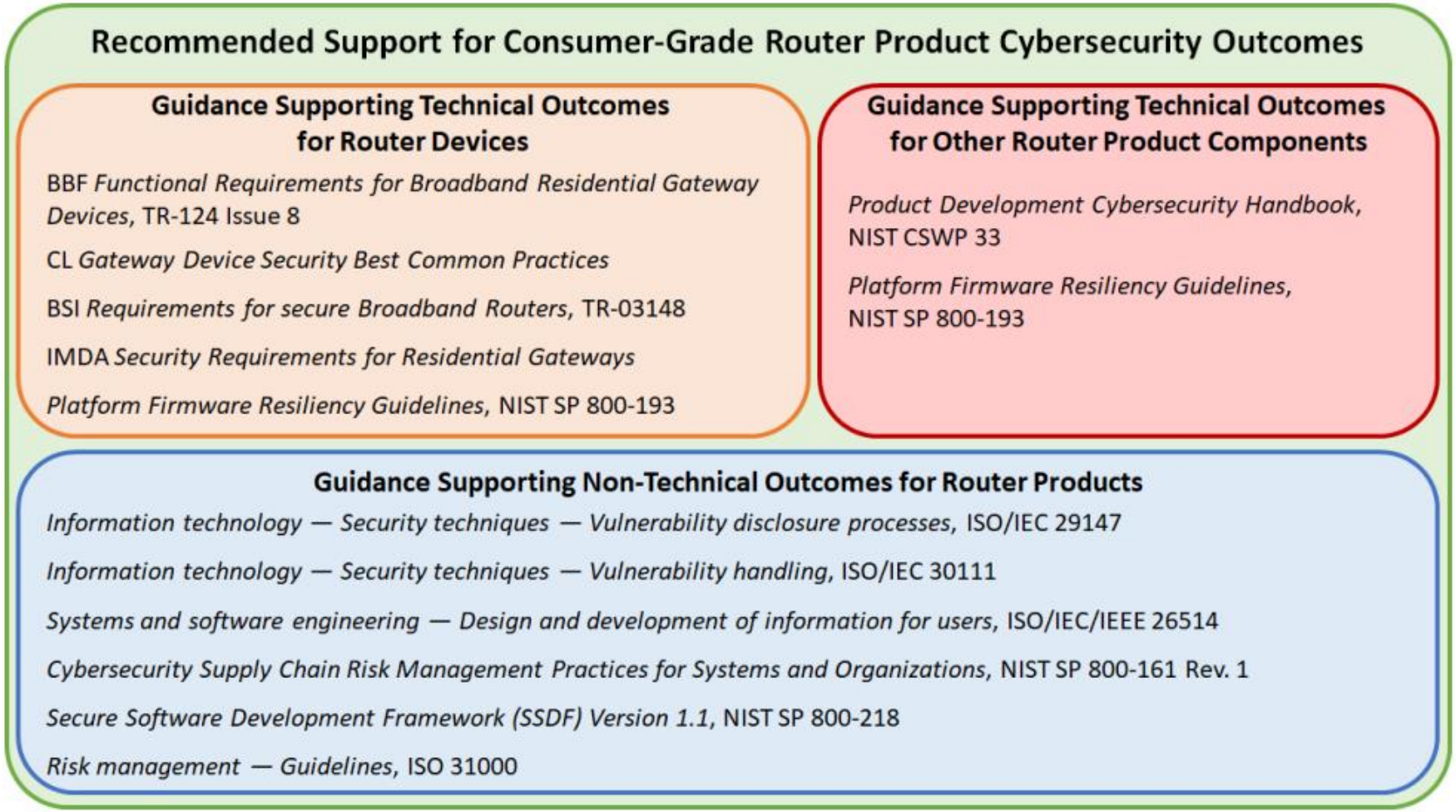




Source: Profile of the IoT Core Baseline for Consumer IoT Products (nist.gov)

NIST 8425A

Recommended Cybersecurity Requirements for Consumer-Grade Router Products



Source: NIST IR 8425A initial public draft, Recommended Cybersecurity Requirements for Consumer-Grade Router Products

EU RED/CRA and EN 303645

EU Cyber Resilience Act

First proposed in 2022, the Cyber Resilience Act introduces mandatory cybersecurity requirements for “products with digital elements” that are sold in the European Union (EU).

The Act recently achieved final agreement to impose full-lifecycle security testing during design and development, harmonize cybersecurity frameworks for hardware and software manufacturers, enhance transparency, and ultimately improve consumer confidence in a phased adoption to start in late 2025.

ETSI EN 303 645

The ETSI EN 303 645 standard establishes a cybersecurity benchmark for consumer IoT devices. It aims to improve IoT security and protect consumer privacy through a detailed framework of 13 key provisions. These provisions cover critical areas like secure communication, data protection, software updates, and resilience against cyber threats, addressing the secure development, deployment, and maintenance of IoT products. By complying with this standard, manufacturers and service providers can significantly reduce the risk of security vulnerabilities, creating a safer environment for consumers and enhancing their trust in IoT devices.

Globally, this standard is now foundational for various national certification schemes, influencing regulations in Finland, Germany, Singapore, India, Vietnam, the UK, and Australia. Efforts to facilitate broader adoption include translations for non-English speaking countries and mutual recognition agreements, like those between Singapore, Finland, and Germany, which promote international cooperation on cybersecurity standards. The World Economic Forum's incorporation of EN 303 645 principles into a global consensus for IoT security measures further highlights its pivotal role in shaping global acceptance. While this standard was initially developed with the EU Cybersecurity Act in mind, its influence extends beyond Europe, and serves as a critical element in the global effort to secure the IoT ecosystem — as both the US and EU have announced plans for mutual recognition of consumer IOT certification.

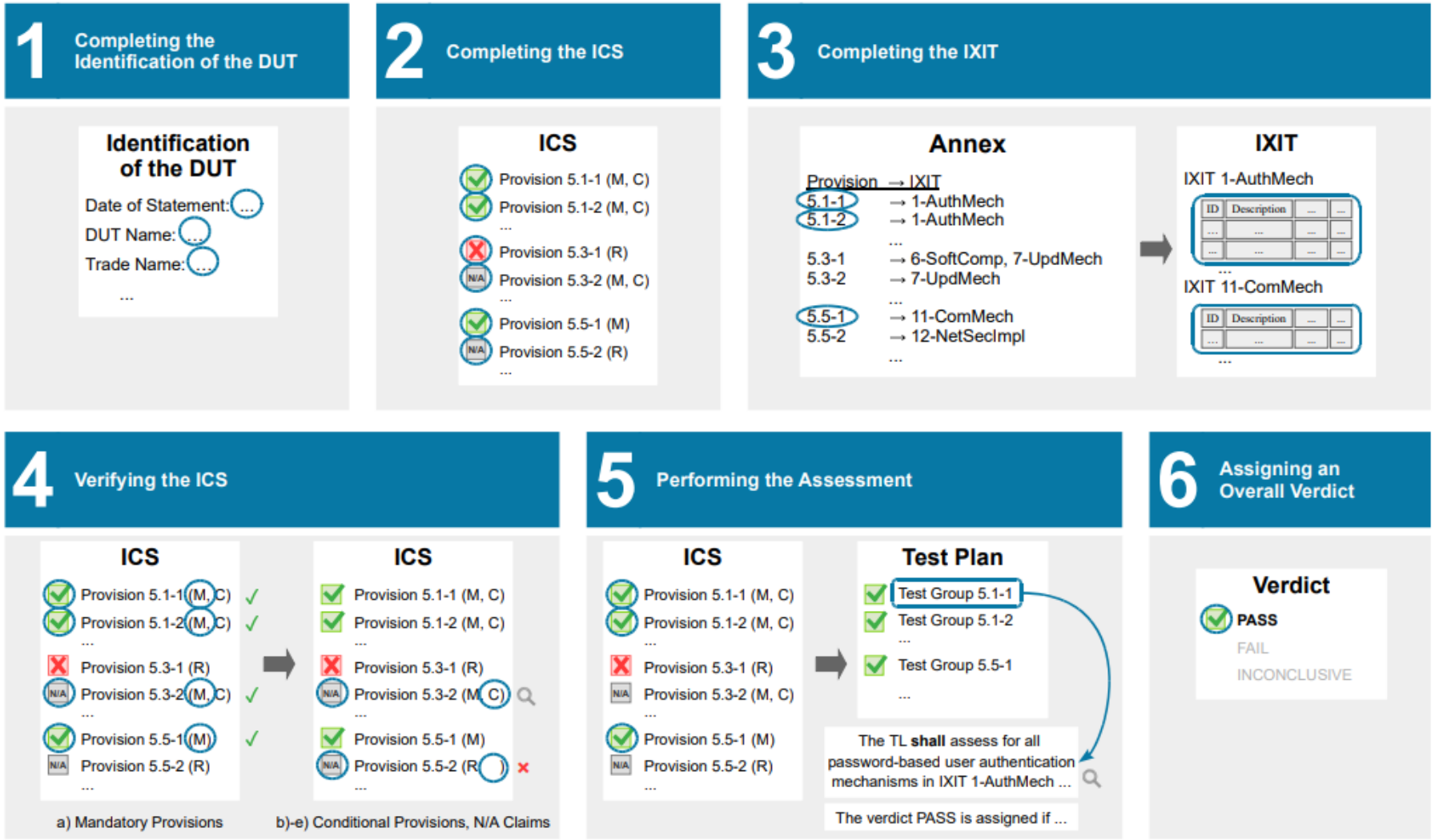
EN 303 645

Checklist

- Password Security
- Vulnerability Disclosure
- Software Updates
- Sensitive Data Storage
- Secure Communications
- Attack Surface Management
- Software Integrity
- Personal Data Security
- Outage Resiliency
- System Telemetry
- User Data Privacy
- Simplified Onboarding and Maintenance
- Input Data validation

Assessment Procedure

ETSI TS 103701

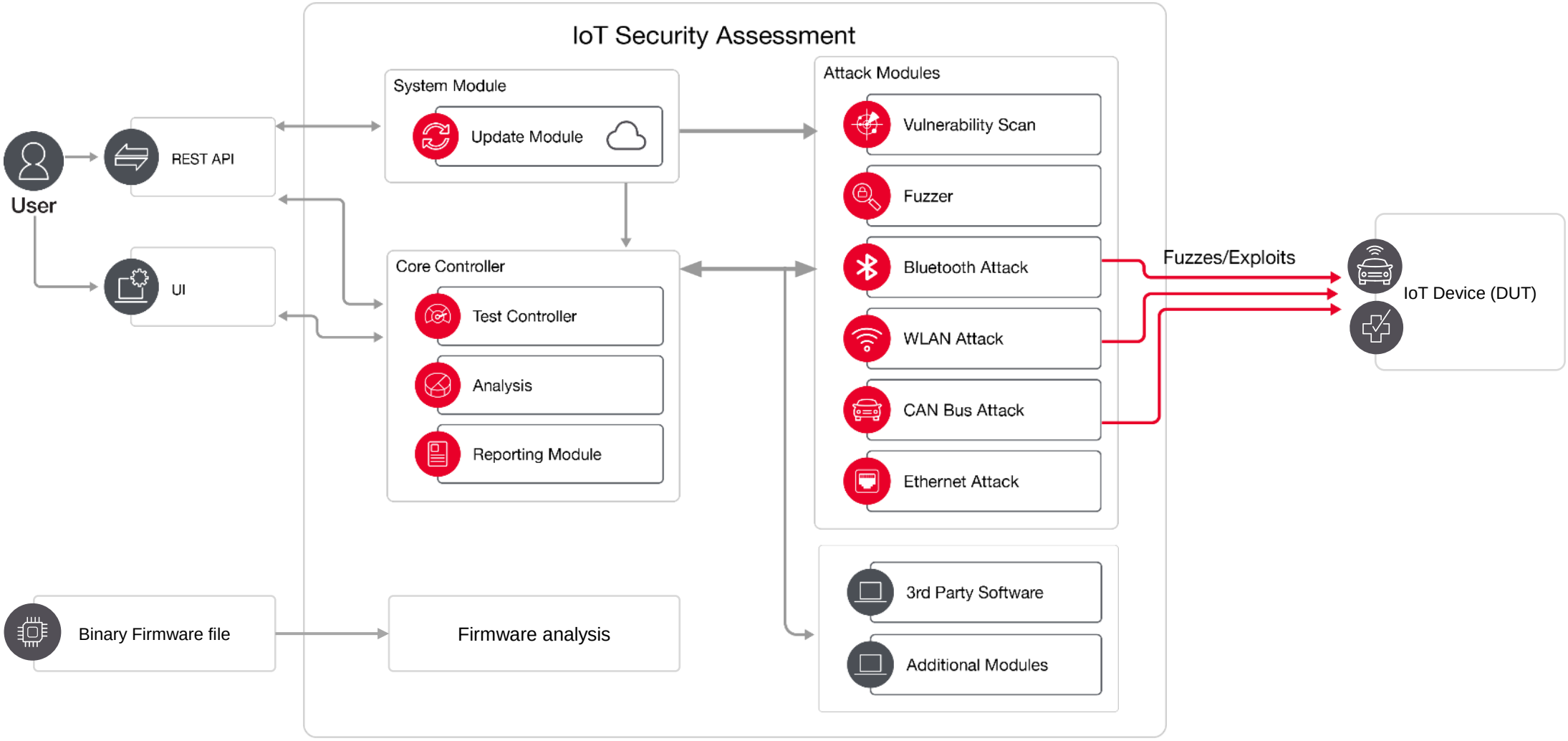


Source: TS 103 701

Solutions

IoT Security Assessment Architecture Overview

High level architecture



Key Firmware Analysis Features

1 Security Analysis

- CVE Detection
- Detection of Hard-Coded Credentials
- Configuration Flaws Analysis
- Analysis of Cryptographic Practices
- Script Vulnerability Identification

2 SBOM Generation SCA

- Identifying open-source components, like embedded OS and libraries.
- Generating Software Bill of Materials (SBOM) automatically in SPDX and CycloneDX formats.
- Supports 400+ key embedded system components, with ongoing updates.

3 Binary Analysis SAST

- Attack surface analysis
- 0-day vulnerability discovery

4 SBOM Generation SCA

30 common firmware formats

- Squashfs
- LZMA
- JFFS2
- UBIFS
- ISO9660
- EXT2
- YAFFS2
- And many more

Resources

物聯網安全風險評估

KEYSIGHT