

CSCI E-11

Class 12

April 21, 2026

IoT Security and Risks



Harvard
Extension School
HARVARD DIVISION OF
CONTINUING EDUCATION

News Story of the Week: Signal message text retrieved by FBI.

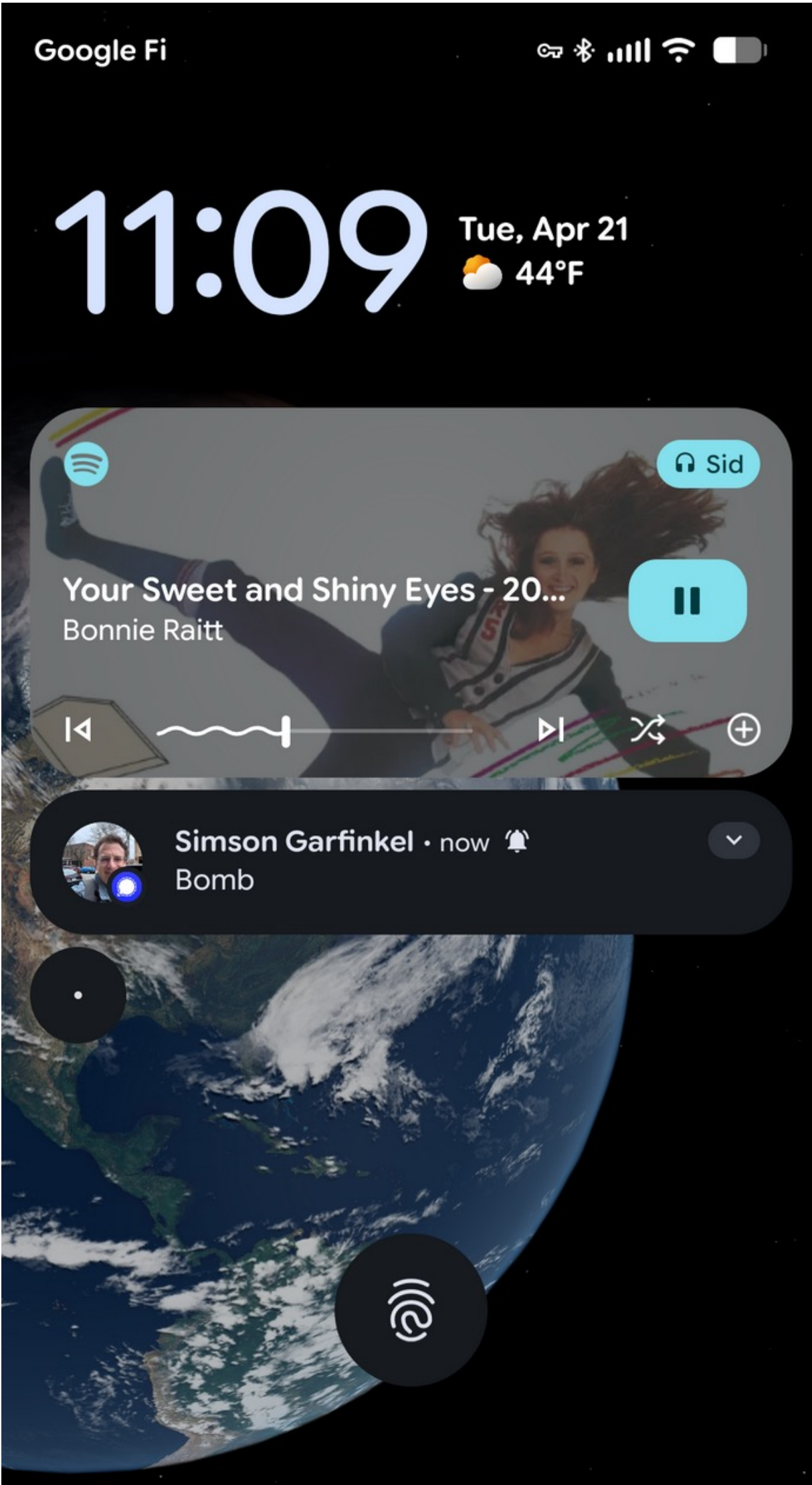
FBI Extracts Suspect's Deleted Signal Messages Saved in iPhone Notification Database

~~404~~

The case was the first time authorities charged people for alleged "Antifa" activities after President Trump designated the umbrella term a terrorist organization.

JOSEPH COX · APR 9, 2026 AT 9:27 AM

<https://www.404media.co/fbi-extracts-suspects-deleted-signal-messages-saved-in-iphone-notification-database-2/>



April 2025: Crosswalk messages hacked.

PARESH DAVE

SECURITY APR 13, 2026 6:38 AM

The Dumbest Hack of the Year Exposed a Very Real Problem

Last April, a hacker hijacked crosswalk announcements to mimic Mark Zuckerberg and Elon Musk. Records obtained by WIRED reveal how unprepared local authorities were.

<https://www.wired.com/story/crosswalk-city-hack-cybersecurity-lessons/>



Reading of the Week: Nizetic

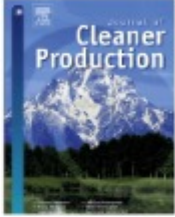
Journal of Cleaner Production 274 (2020) 122877

ELSEVIER

Contents lists available at ScienceDirect

Journal of Cleaner Production

journal homepage: www.elsevier.com/locate/jclepro



Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future



Sandro Nizetić ^{a,*}, Petar Šolić ^b, Diego López-de-Ipiña González-de-Artaza ^c, Luigi Patrono ^d

^a LITEF-Laboratory for Thermodynamics and Energy Efficiency, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Rudjera Boskovicica 32, 21000, Split, Croatia
^b Department of Electronics, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, University of Split, Rudjera Boskovicica 32, 21000, Split, Croatia
^c Faculty of Engineering, DeustoTech - Fundación Deusto, Universidad de Deusto, Despacho 545 Avda, Universidades 24, 48007, Bilbao, Spain
^d Department of Innovation Engineering, University of Salento, Ecotekne Campus - S.P. 6, Lecce, Monteroni, 73100, LECCE, LE, Italy

ARTICLE INFO

Article history:
Received 11 May 2020
Received in revised form 12 June 2020
Accepted 13 June 2020
Available online 19 July 2020

Handling editor: Cecilia Maria Villas Boas de Almeida

Keywords:
IoT
Smart city
Sustainability
Energy
Environment
SpliTech2020

ABSTRACT

The rapid development and implementation of smart and IoT (Internet of Things) based technologies have allowed for various possibilities in technological advancements for different aspects of life. The main goal of IoT technologies is to simplify processes in different fields, to ensure a better efficiency of systems (technologies or specific processes) and finally to improve life quality. Sustainability has become a key issue for population where the dynamic development of IoT technologies is bringing different useful benefits, but this fast development must be carefully monitored and evaluated from an environmental point of view to limit the presence of harmful impacts and ensure the smart utilization of limited global resources. Significant research efforts are needed in the previous sense to carefully investigate the pros and cons of IoT technologies. This review editorial is partially directed on the research contributions presented at the 4th International Conference on Smart and Sustainable Technologies held in Split and Bol, Croatia, in 2019 (SpliTech 2019) as well as on recent findings from literature. The SpliTech2019 conference was a valuable event that successfully linked different engineering professions, industrial experts and finally researchers from academia. The focus of the conference was directed towards key conference tracks such as Smart City, Energy/Environment, e-Health and Engineering Modelling. The research presented and discussed at the SpliTech2019 conference helped to understand the complex and intertwined effects of IoT technologies on societies and their potential effects on sustainability in general. Various application areas of IoT technologies were discussed as well as the progress made. Four main topical areas were discussed in the herein editorial, i.e. latest advancements in the further fields: (i) IoT technologies in Sustainable Energy and Environment, (ii) IoT enabled Smart City, (iii) E-health – Ambient assisted living systems (iv) IoT technologies in Transportation and Low Carbon Products. The main outcomes of the review introductory article contributed to the better understanding of current technological progress in IoT application areas as well as the environmental implications linked with the increased application of IoT products.

© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

With rising technological developments in society, new possibilities have occurred and that could simplify our daily life and provide more efficient services or production processes.

Digitalization has allowed “smart” (Zheng et al., 2019) to become the epicentre of already ongoing technological developments. In fact, IoT technologies are nowadays assumed to be one of the key pillars of the fourth industrial revolution due to significant potential in innovations and useful benefits for the population. On the other side, each development utilizes limited resources leaving behind different environmental footprints, (Li et al., 2020a), especially different kinds of pollutants, (Zeinalnezhad et al., 2020). Internet of things (IoT) based technologies bring a completely new

* Corresponding author.
E-mail address: snizetic@fesb.hr (S. Nizetić).

IoT: Utopia or Necropolis?



Why is IoT security important?



IoT devices can be beachheads into more secure networks.

FINANCE

Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank

By [Oscar Williams-Grut](#)



An aquarium at a casino — but not the one in question. [Ethan Miller/Getty Images](#)

Apr 15, 2018, 3:08 AM ET

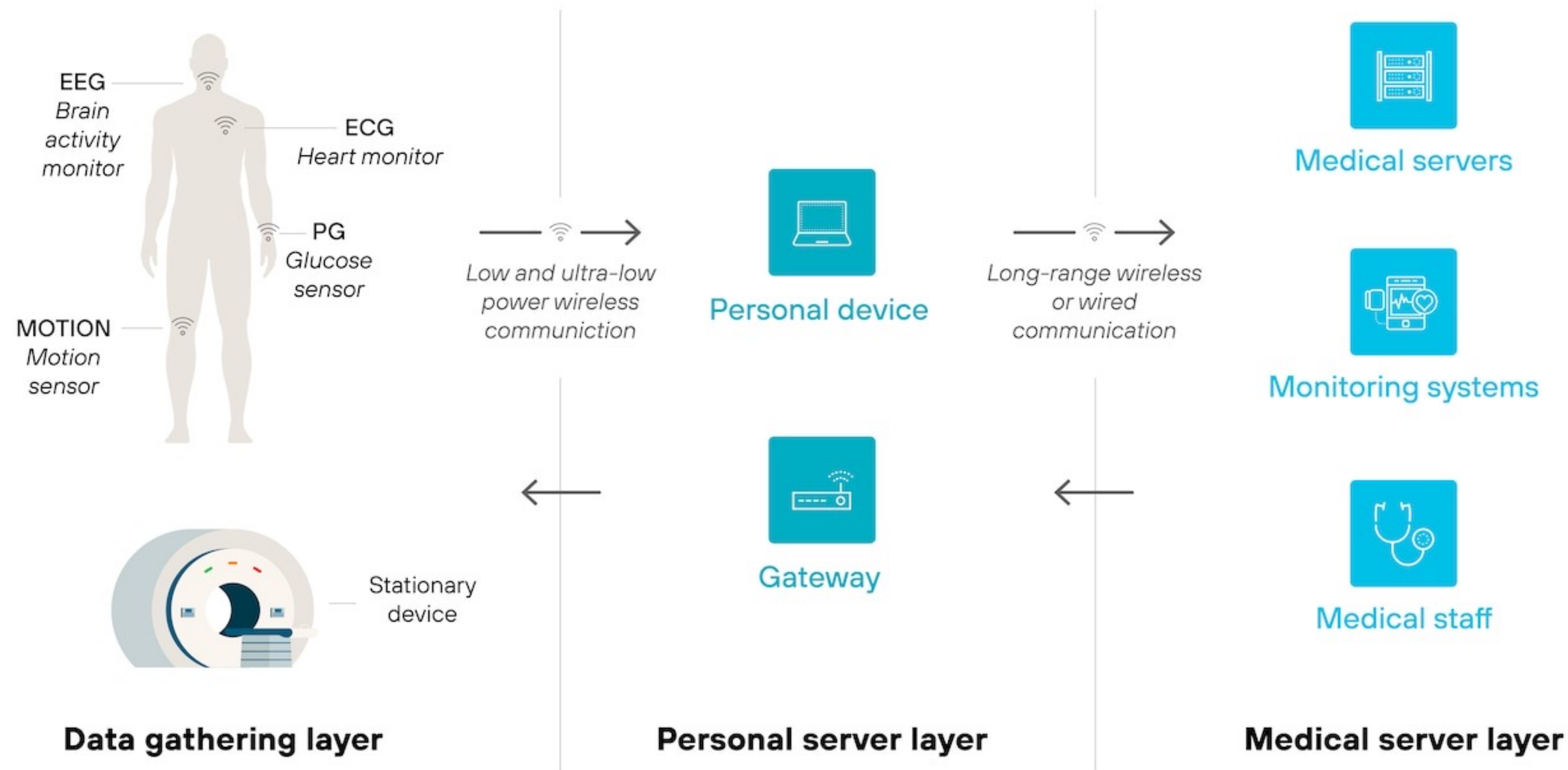
[Share](#) [Save](#)

IoT devices can be placed in sensitive or private locations.



Internet-connected devices are used in healthcare, even embedded in our bodies.

Internet of Medical Things (IoMT) architecture



In 2013, Barnaby Jack hacked a pacemaker remotely to generate a lethal shock.



Have things improved since then?



Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

TLP:WHITE

12 September 2022

PIN Number
20220912-001

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS/CISA.

This PIN has been released **TLP:WHITE**

- As of January 2022, a research report conducted by a cybersecurity firm found 53% of connected medical devices and other internet of things (IoT) devices in hospitals had known critical vulnerabilities. Approximately one third of healthcare IoT devices have an identified critical risk potentially implicating technical operation and functions of medical devices.
- According to a research report in 2021, a cybersecurity firm assessed there is an average of 6.2 vulnerabilities per medical device, and recalls were issued for critical devices such as pacemakers and insulin pumps with known security issues, while more than 40% of medical devices at the end-of-life stage offer little to no security patches or upgrades.

Did we learn anything? Maybe.

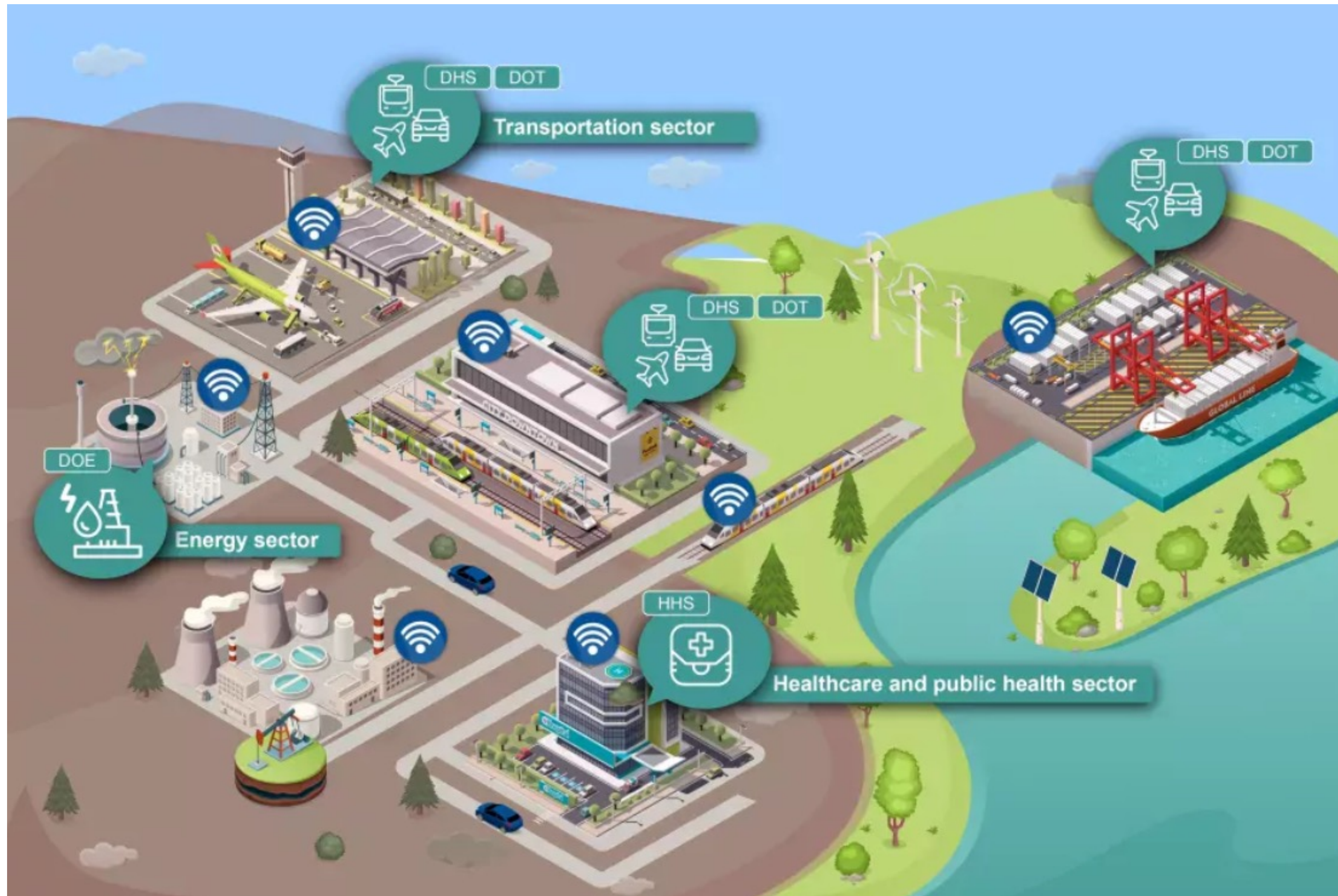
POLITICS • 4 MIN READ

Pro-Iran hackers claim cyberattack on major US medical device maker

UPDATED MAR 15, 2026 ▾

By  Sean Lyngaas

Internet-connected Critical Infrastructure is another serious threat to safety.

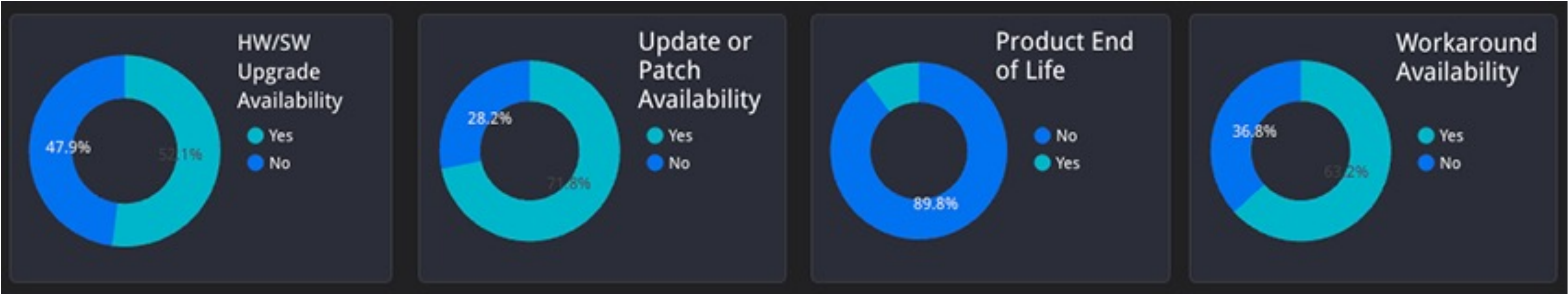
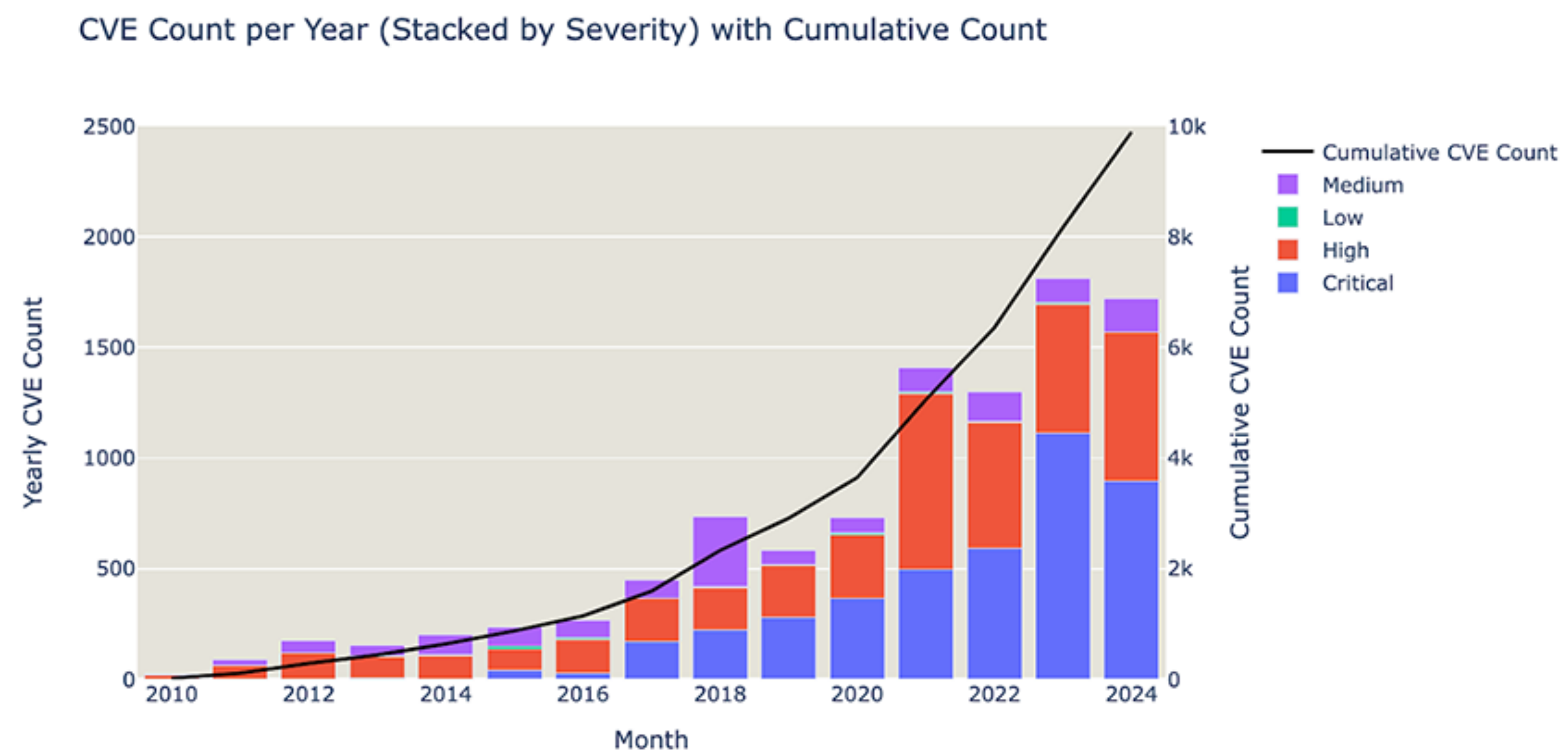


2021 ransomware attack paralyzed Colonial Pipeline, leading to gas shortages.



<https://www.nytimes.com/2021/05/10/business/colonial-pipeline-ransomware.html>

Count of known CVEs affecting CI are increasing, many with no patch available.



Embedded processors are still under attack.

**JOINT
CYBERSECURITY
ADVISORY**

TLP: CLEAR

Co-Authored by:

Product ID: AA26-097A



**Iranian-Affiliated Cyber Actors
Exploit Programmable Logic
Controllers Across US Critical
Infrastructure**

The Internet of Broken Things



This is how the internet of things will work. All the things will be interesting. We will think we own them because we will have bought them. But we won't own all the pieces that give them utility.

The pieces will include some service that promised to provide value unless you read the fine print. Companies will be bought and sold. Databases will accumulate mistakes. Things will stop working. The compounding of complexity will make it in no ones interest to go fix the thing, even if it is just one line missing.

Ward Cunningham, 2014

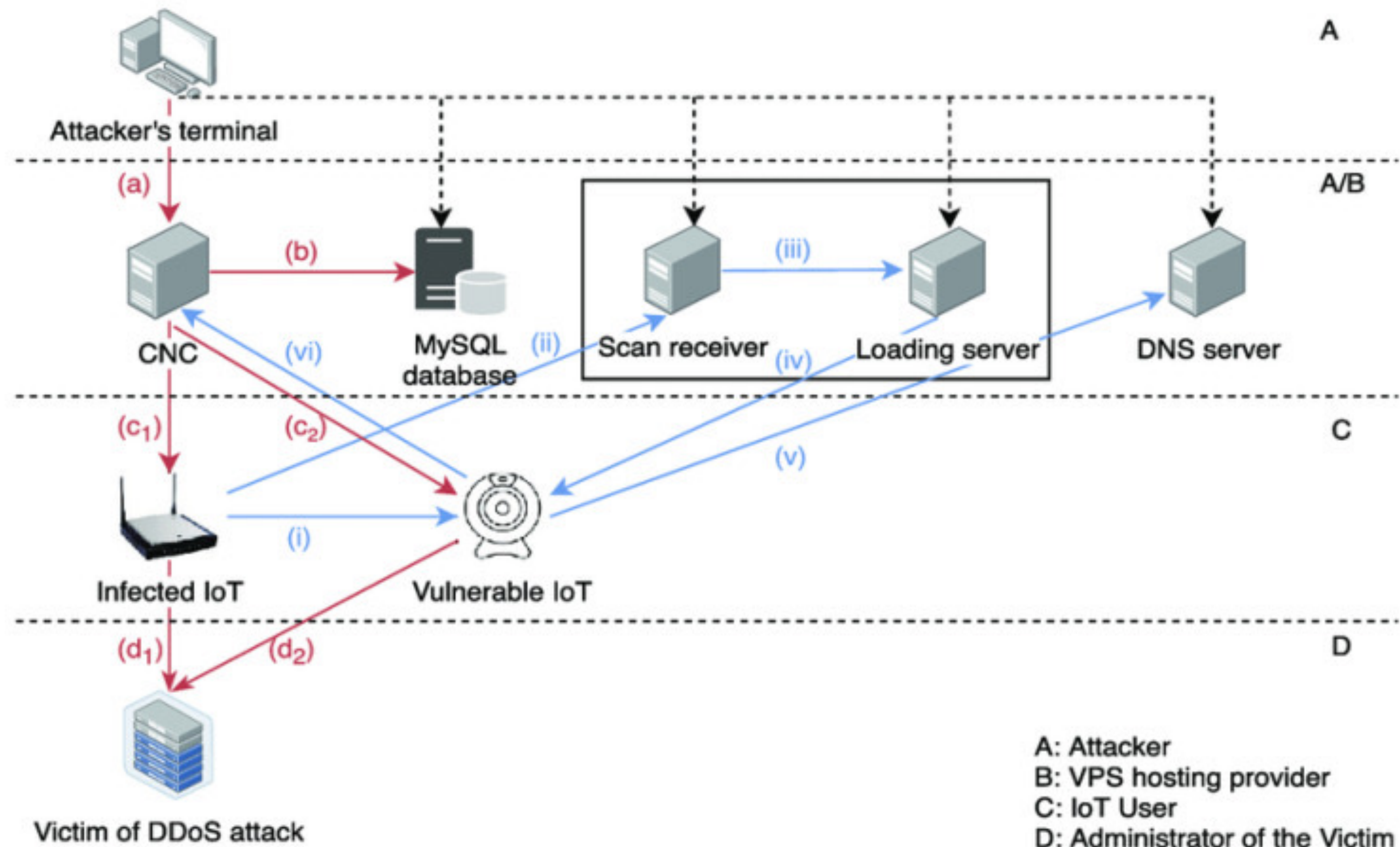
<https://hapgood.us/2016/10/21/internet-of-broken-things/>

What do you do when your IoT devices stop working? You throw them out.



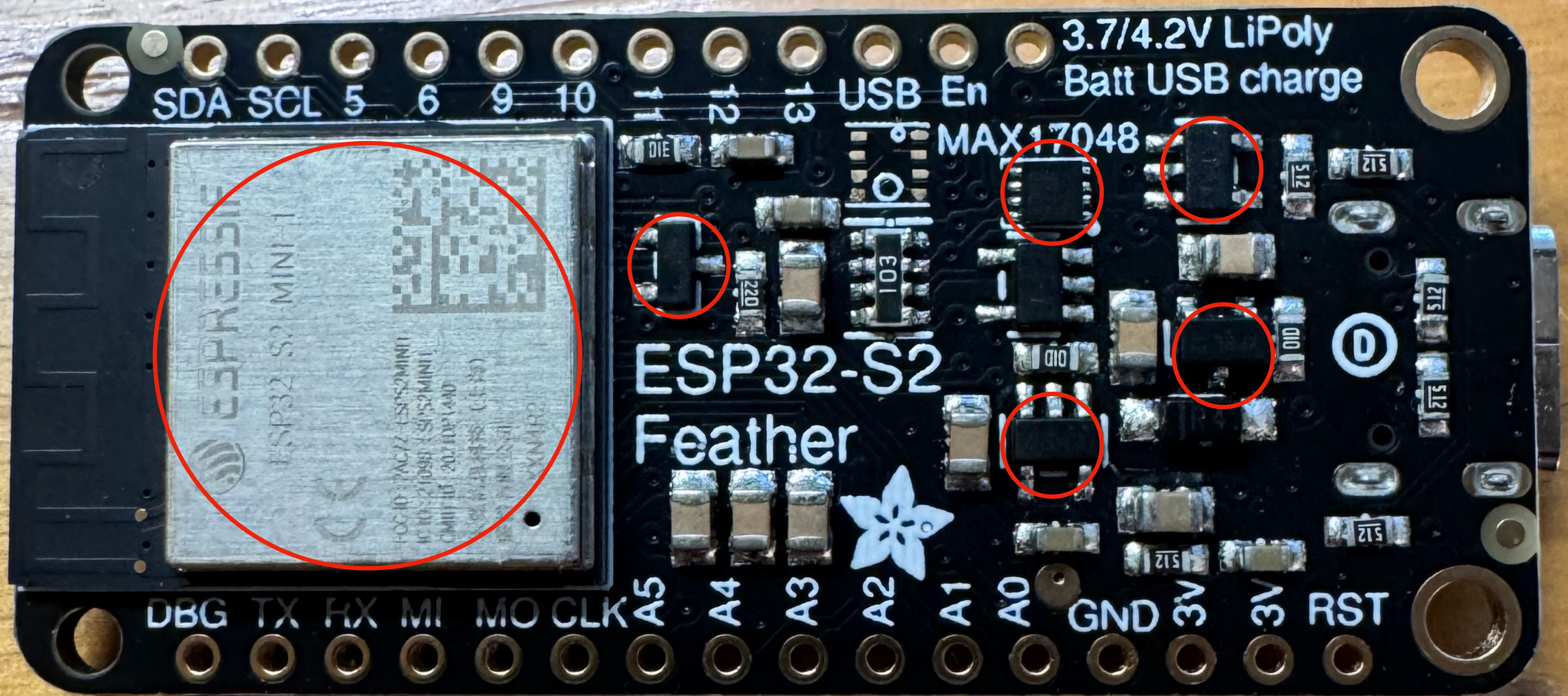
Compromised IoT devices serve as infrastructure for botnet DDoS attacks.

Architecture of the Mirai botnet



IoT Physical Attacks

Q: What if you could “edit” a silicon chip?



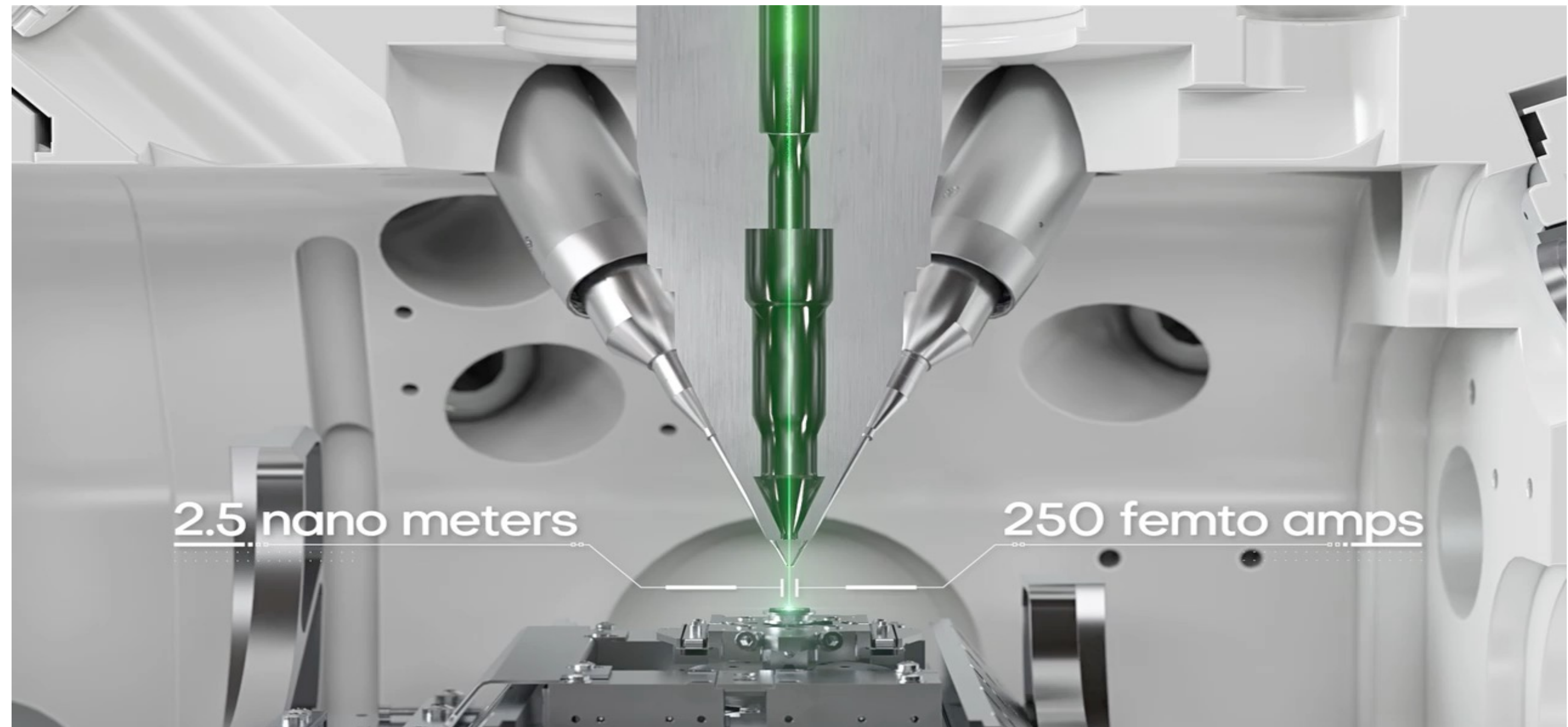
Chip editing is real.

ThermoFisher
SCIENTIFIC

FIB Circuit Edit
FIB circuit edit and semiconductor
prototyping.

Contact us

Join the Conversation



<https://www.thermofisher.com/us/en/home/semiconductors/circuit-edit.html/1000>

“Chip Off”



Forensic Science International: Digital Investigation

Volumes 42–43, October–December 2022, 301481



Cheap as chips: An accessible chip off acquisition method for ball grid array (BGA) integrated circuits in digital investigations

M. Hadgkiss  , S. Morris, S. Paget, A. Ventress, K. Norris

Show more 

 Add to Mendeley  Share  Cite

<https://doi.org/10.1016/j.fsidi.2022.301481>

[Get rights and content](#)

Under a Creative Commons [license](#)

 Open access

<https://www.sciencedirect.com/science/article/pii/S2666281722001627>

Chip Off Methodology

Deconstruction

- Research available resources
- Source replica device
- Open outer casings
- Free the PCB



Perform



- Perform suitable data reading methods.

Determine

- Determine BGA number
- Research and select suitable data reading methods.



Restoration

- Secure the IC and apply flux
- Use solder wick and iron to remove solder
- Apply isopropyl alcohol
- Re solder the pads



Removal

- Secure the PCB
- Set up equipment
- Apply hot air to IC
- Use removal tool to separate the IC from the PCB



Identification



- Identify data storage IC
 - If needed, file EM shielding

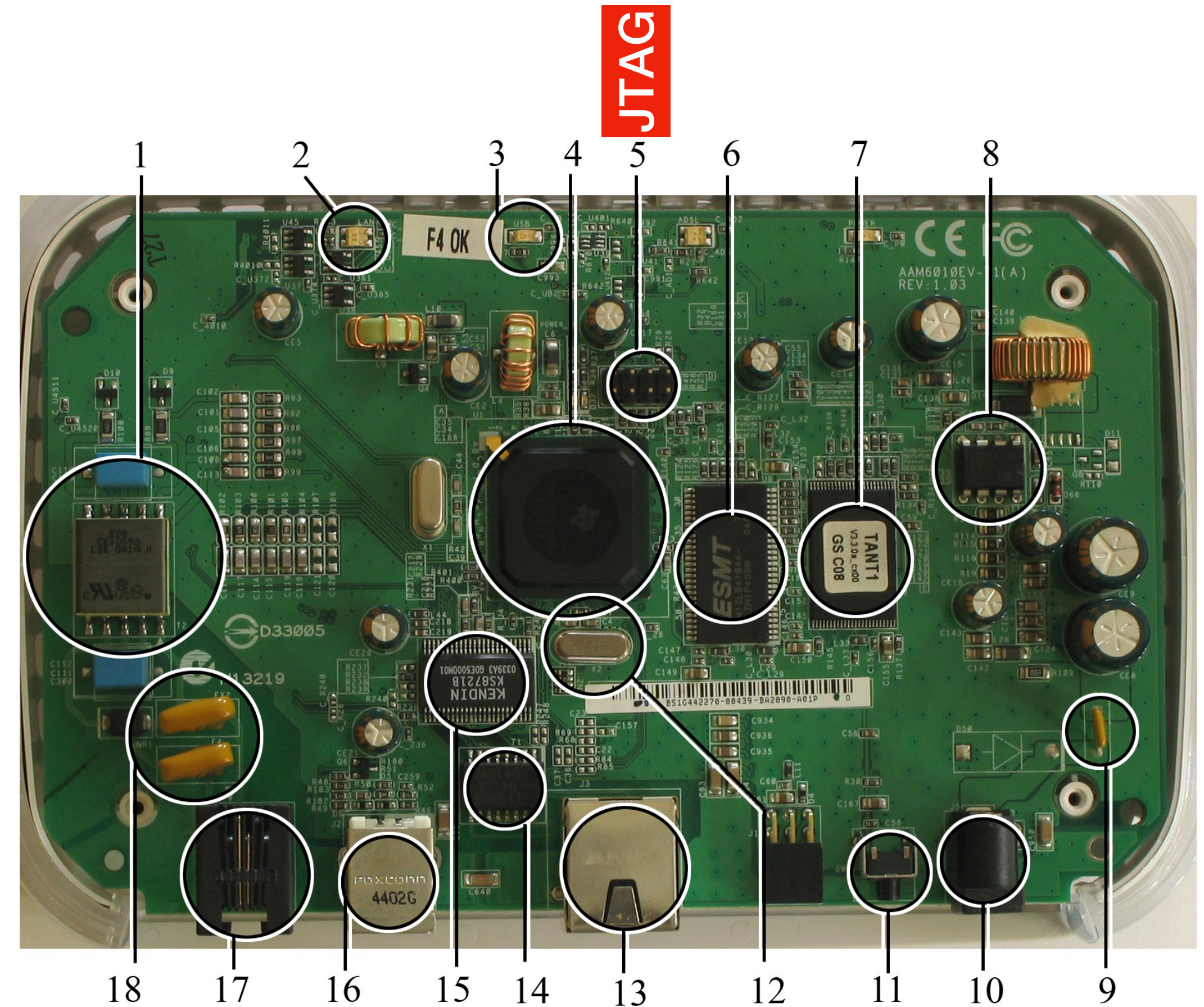
Joint Test Action Group (JTAG) — a universal hardware back door



Netgear DG632 ADSL Router

•JTAG uses:

- Read memory
- Write memory
- Exercise hardware



Internal circuit board.

ESP32 (Memento processor) supports JTAG.

Debugging ESP32 App with ESP-PROG

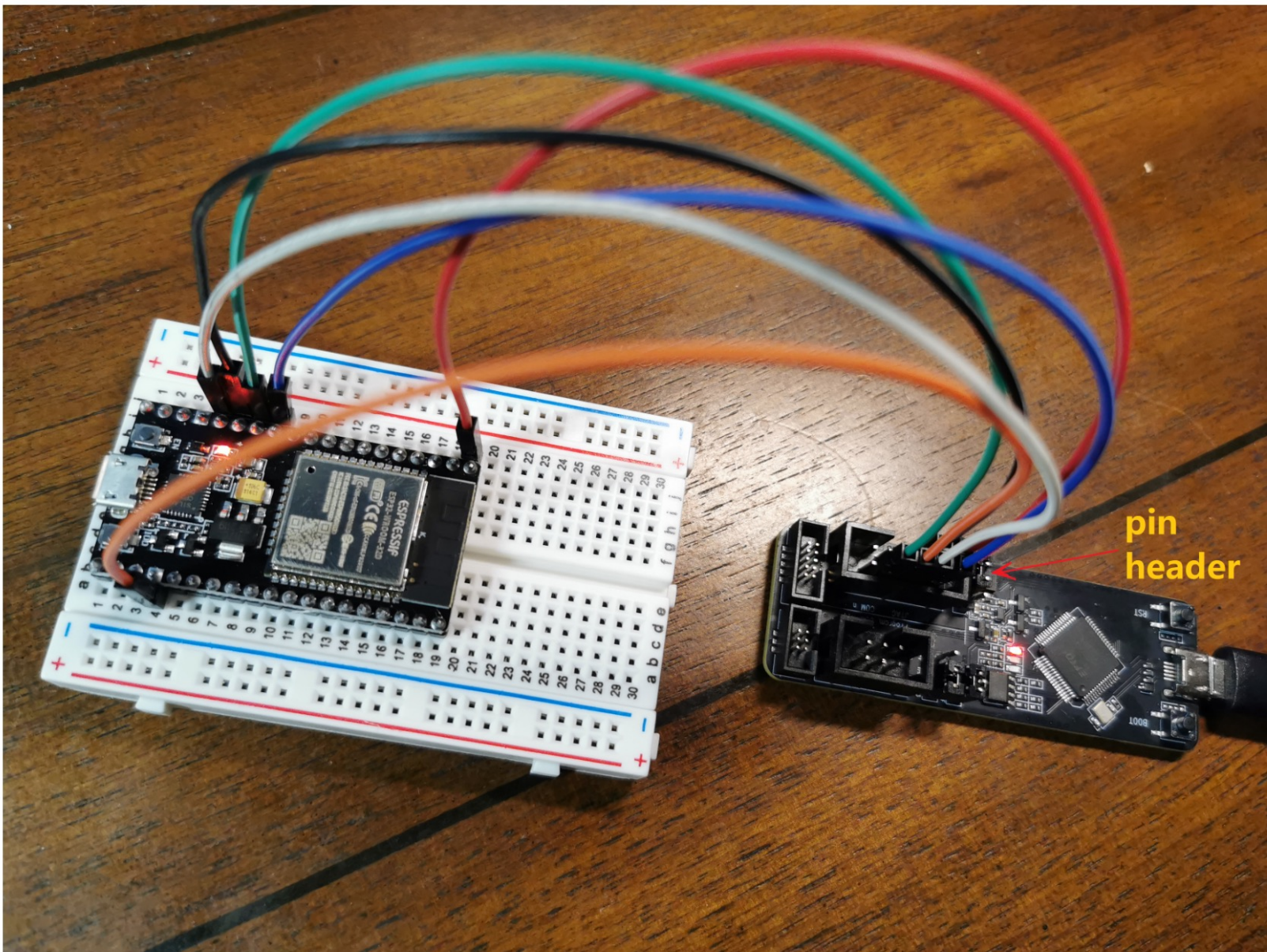
Debug your embedded software with ESP32, ESP-PROG, and JTAG. This project is part of a course at University of Massachusetts Lowell, and some details may need to be changed to work for other readers.

The ESP32 app in this project sets up the ESP32 board as a WiFi access point with SSID of *fxw* and password of *xinwenfu*.

Overview

The ESP32 supports the JTAG debugging interface, which can allow users to debug their embedded applications through GDB much like they would debug a normal Windows/Linux executable. For instance, JTAG allows users to place breakpoints in code, view the memory stack, view registers, and more. However, most ESP32 boards on the market do not contain the required hardware for communicating with an external JTAG adapter. This hardware can be found on chips such as FT2232HL, which is implemented by the ESP-PROG. Other technical details will be spared here. You may refer to Espressif's guides on [JTAG debugging](#) and [ESP-PROG](#) for more information on these topics.

See below for a look at how the Hiletgo ESP-WROOM-32 board may connect to ESP-PROG:



<https://github.com/PBearson/ESP32-With-ESP-PROG-Demo>

JTAG Debugging

[\[中文\]](#)

This document provides a guide to installing OpenOCD for ESP32 and debugging using GDB.

Note

You can also debug your ESP32 without needing to setup JTAG or OpenOCD by using `idf.py monitor`. See: [IDF Monitor](#) and [CONFIG_ESP_SYSTEM_GDBSTUB_RUNTIME](#).

The document is structured as follows:

Introduction

Introduction to the purpose of this guide.

How it Works?

Description how ESP32, JTAG interface, OpenOCD and GDB are interconnected and working together to enable debugging of ESP32.

Selecting JTAG Adapter

What are the criteria and options to select JTAG adapter hardware.

Setup of OpenOCD

Procedure to install OpenOCD and verify that it is installed.

Configuring ESP32 Target

Configuration of OpenOCD software and setting up of JTAG adapter hardware, which together make up the debugging target.

Launching Debugger

Steps to start up a debug session with GDB from [Eclipse](#) and from [Command Line](#).

Debugging Examples

If you are not familiar with GDB, check this section for debugging examples provided from [Eclipse](#) as well as from [Command Line](#).

Building OpenOCD from Sources

Procedure to build OpenOCD from sources for [Windows](#), [Linux](#) and [macOS](#) operating systems.

Tips and Quirks

This section provides collection of tips and quirks related to JTAG debugging of ESP32 with OpenOCD and GDB.

tomorrow
belongs to those who embrace it
today

trending

tech

innovation

business

security

advice

buying g

/ tech

Home / Tech / Smartphones / Mobility

For \$15,000, GrayKey promises to crack iPhone passcodes for police

This palm-sized box can break your iPhone's password, giving police full access to a device's file system -- messages, photos, call logs, browsing history, keychain and user passwords, and more.

Written by Zack Whittaker, Contributor

March 19, 2018 at 12:32 p.m. PT

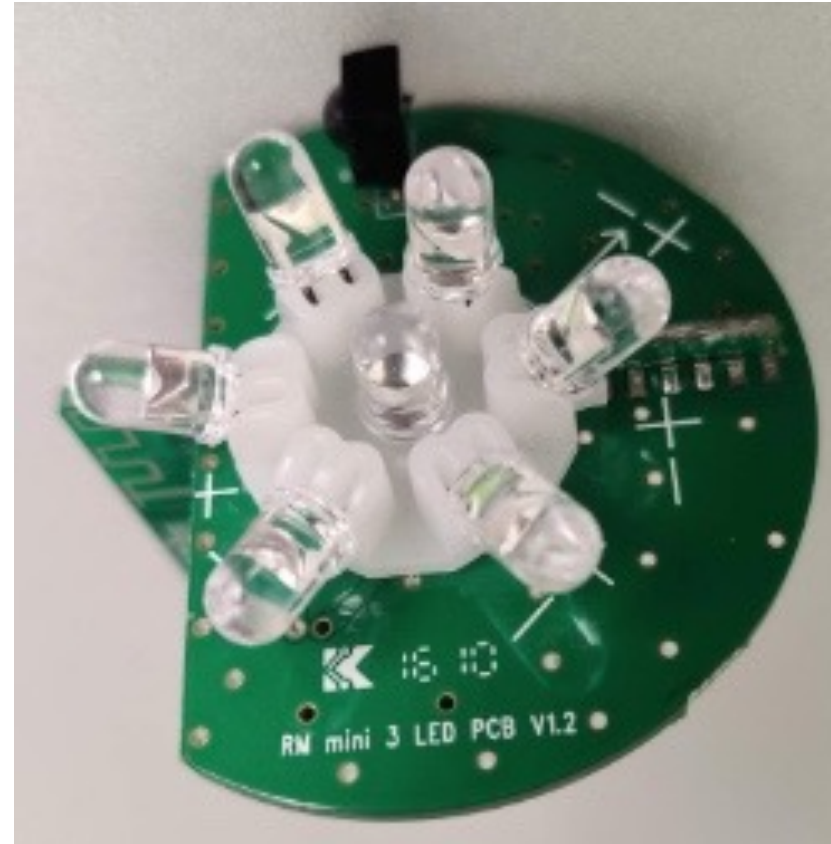
in

f

<https://www.zdnet.com/article/graykey-box-promises-to-unlock-iphones-for-police/>

A black, palm-sized GrayKey device is shown. It has two white Lightning cables plugged into its front ports. The word "Status" is visible on the front panel. The device is sitting on a light-colored surface.

You can extract Wi-Fi passwords from IoT device memory.

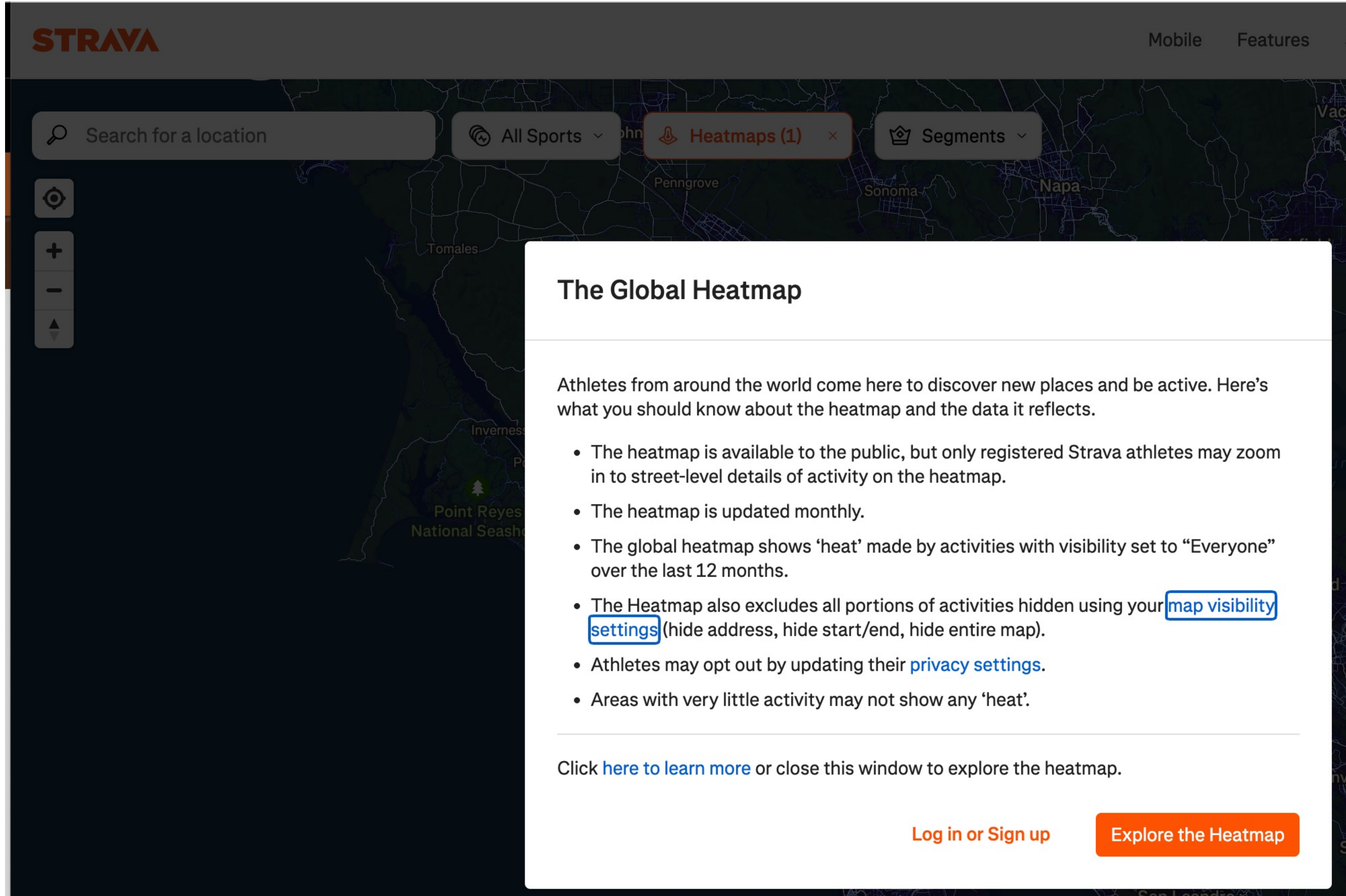


```
broadlink Hello World application Started Product Type :10039 V20027
[partition] Error: Partition Table 1 @0x2000 is corrupted
[sdio] Card detected
[sdio] Card reset successful
[sdio] Card Version - (0x32)
[sdio] Card initialization successful
[wlcm] WLAN FW ext_version: w8801-B0, RF878X, FP68, 0.0.0.p16
[af] app_ctrl: reset_to_factory=0, prev_fw_version=1
[wlcm] SUPP EVENT = 0 data = 0x00000000 len=0
[net] Initializing TCP/IP stack
```

```
app_firmware_start startup success.
task_thread startup success.
,,,,,,,,,bl2_thread,,,,,,,,,
ssid WirelessSSID psk WirelessPassw0rd need broad 0
type 3
ssid WirelessSSID psk WirelessPassw0rd psklen 16, type 5 special 0
app_network_status_set to status. 6.....
[af] app_ctrl: Connecting to the loaded network
```


IoT Privacy Attacks

Strava Heatmaps showed where people were running.



STRAVA Mobile Features S

Search for a location

All Sports  **Heatmaps (1)**  Segments 



The Global Heatmap

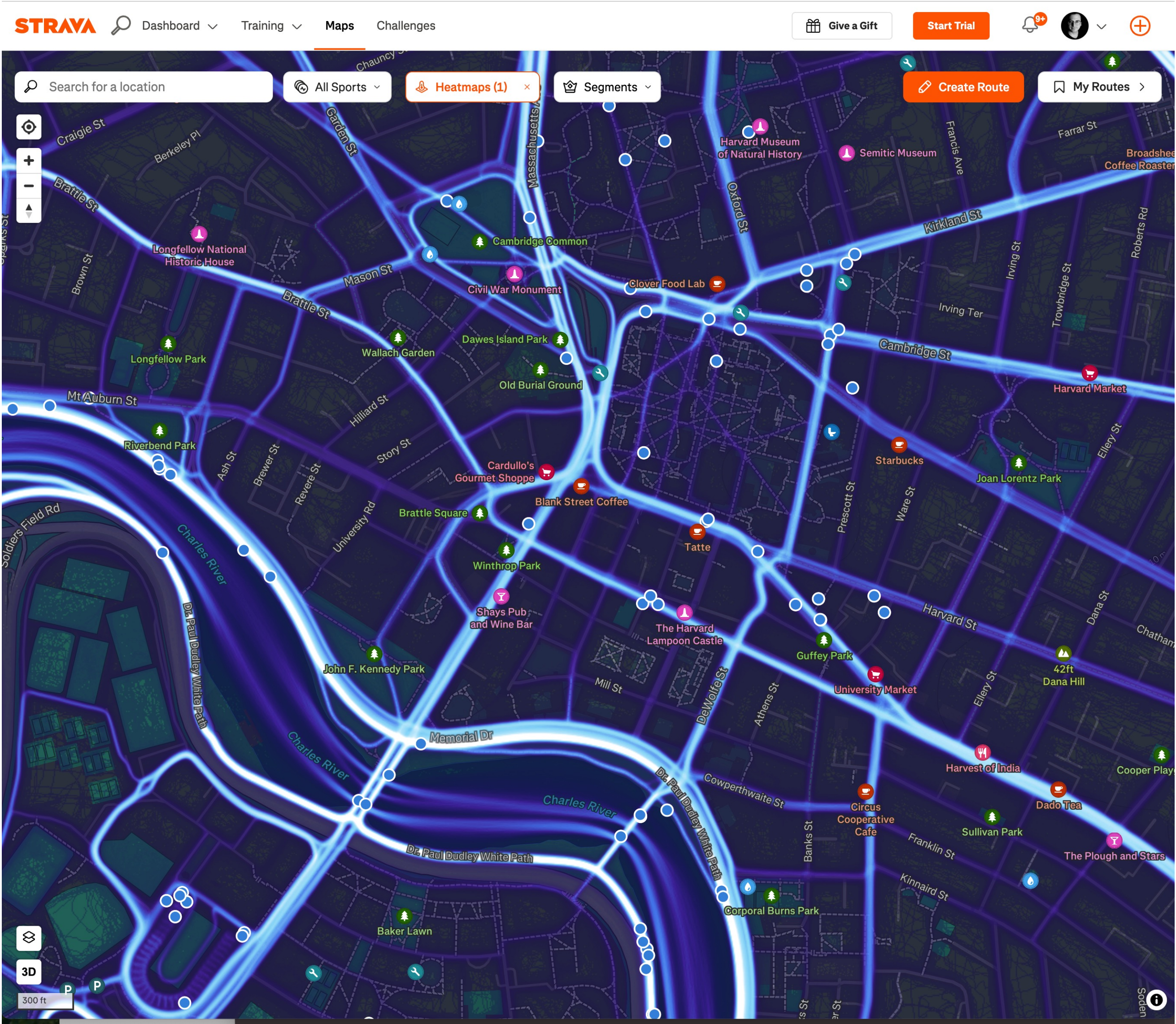
Athletes from around the world come here to discover new places and be active. Here's what you should know about the heatmap and the data it reflects.

- The heatmap is available to the public, but only registered Strava athletes may zoom in to street-level details of activity on the heatmap.
- The heatmap is updated monthly.
- The global heatmap shows 'heat' made by activities with visibility set to "Everyone" over the last 12 months.
- The Heatmap also excludes all portions of activities hidden using your [map visibility settings](#) (hide address, hide start/end, hide entire map).
- Athletes may opt out by updating their [privacy settings](#).
- Areas with very little activity may not show any 'heat'.

Click [here to learn more](#) or close this window to explore the heatmap.

[Log in or Sign up](#) [Explore the Heatmap](#)

Anonymized, unlabeled data showed patterns of use.



Heatmap revealed location of and streetmap of military base in Afghanistan.

Fitness app Strava lights up staff at military bases

29 January 2018

Share  Save 



The movements of soldiers within Bagram air base - the largest US military facility in Afghanistan

Security concerns have been raised after a fitness tracking firm showed the exercise routes of military personnel in bases around the world.

Online fitness tracker Strava has published a "heatmap" showing the paths its users log as they run or cycle.

It appears to show the structure of foreign military bases in countries including Syria and Afghanistan as soldiers move around them.

The US military was examining the heatmap, a spokesman said.

B B C

Alexa, testify!

Amazon’s First Amendment Arguments in its Response to a Subpoena for a Murder Suspect’s Echo Recordings are Punted for Another Day, Another Case

MARCH 27, 2017 STEPHANIE F. KESSLER COMMUNICATIONS/MEDIA, ALEXA, BUSINESS LITIGATION, STEPHANIE FRANXMAN, DAYTON LAW FIRM, AMAZON, CINCINNATI LAWYER, FIC BLOG, CINCINNATI LAW FIRM, ECHO



On February 17, 2017, Amazon filed a 91-page memorandum of law in support of its motion to quash a subpoena by Bentonville Arkansas police in a murder investigation. Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant, State of Arkansas v. James Bates, No. CR-2016-370-2 (Ark. Cir. Feb. 17, 2017). The issue of whether or not Amazon would turn over the recordings from the murder suspect's Amazon Echo (also known as Alexa) was resolved when the suspect agreed to turn over the recordings to the police. Elliott C. McLaughlin, *Suspect Oks Amazon to hand over Echo recordings in murder case*, CNN (March 7, 2017, 11:50 AM). Amazon's memorandum of law raises First Amendment concerns that are likely to resurface in later cases given the prevalence of this type of technology.

Background: Arkansas Hot Tub Murder and What Alexa Actually Records

On the morning of November 22, 2015, a man named Victor Collins was found dead in a back patio hot tub at the residence of James Bates. Amazon's Memorandum, Exhibit B Affidavit for Search Warrant. According to police, Victor Collins, James Bates and two other friends had been drinking and watching an Arkansas Razorback football game on the night of November 21, 2015. Id. James Bates, the murder suspect and the owner of the Echo in question, went to bed at 1:00 AM, leaving Victor Collins and one other friend outside in the hot tub. Id. Bates woke up the next morning, found the body of Victor Collins, and called the police. Id. According to James Bates' attorney, Kathleen Zellner (an attorney for Steve Avery who appears in Netflix's "Making a Murderer"), James is innocent. Elliott C. McLaughlin, *Suspect Oks Amazon to hand over Echo recordings in murder case*.

Hidden cameras

TRIPPED UP

Help! We Found a Hidden Camera in the Bathroom of Our Airbnb.

When a couple alerted Airbnb to a spy cam in an outlet extender, they thought the listing would be yanked and they'd get a full refund. Wrong on both counts.

An update on our policy on security cameras

By [Airbnb](#) · March 11, 2024 · [Company](#)

Does Your Airbnb Have Hidden Cameras? Here's How to Check

Though Airbnb has banned indoor cameras, that won't stop unscrupulous hosts. Here's what to do, before and after you book, to make sure you're not being subject to surveillance.



By [Chandra Steele](#) Updated May 21, 2025



(Credit: Credit: Shutterstock/Pixel-Shot, Mulad Images)

Smart glasses raise additional privacy concerns.

'Dystopian'? Smart glasses may be watching (and recording) you

Advocacy groups issued a letter saying the wearable tech represents a “dystopian privacy invasion.” Secret recordings made on the devices have left some people feeling violated.



N'dea Yancey-Bragg
USA TODAY

Updated April 19, 2026, 7:37 p.m. ET



Smart glasses raise concerns about privacy and consent to be recorded

Smart glasses raise new privacy and consent questions as wearable cameras become harder to detect in public spaces.

NIST Attack Analysis

NIST analyzed many IoT vulnerability scenarios with the MITRE ATT&CK.

MITRE | ATT&CK®

Matrices ▼Tactics ▼Techniques ▼Defenses ▼CTI ▼Resources ▼BenefactorsBlog ↗

Search Q

ATT&CK v17 has been released! Check out the [blog post](#) for more information.

ATT&CK®

Get Started

Take a Tour

Contribute

Blog ↗

FAQ

Random Page | ▼

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world – by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

layout: side ▼show sub-techniqueshide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	33 techniques	9 techniques	17 techniques	18 techniques	9 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (3)
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Limitation (3)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternate Protocol (3)
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over Channel (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Network Media (3)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (5)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Media (3)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Input Injection	Create Account (3)	Domain or Policy Modification (2)	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Service (3)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Inter-Process Communication (3)	Create or Modify System Process (5)	Escape to Host	Domain or Tenant Policy Modification (2)	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Exfiltration Over Service (3)
Search Open Websites/Domains (3)		Trusted Relationship	Scheduled Task/Job (5)	Event Triggered Execution (17)	Event Triggered Execution (17)	Execution Guardrails (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (5)	Hide Infrastructure	Schedule Transfer (3)
Search Victim-Owned Websites		Valid Accounts (4)	Serverless Execution	Exclusive Control	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer	Transfer Data to Cloud Account (3)
		Wi-Fi Networks	Shared Modules	External Remote Services	Hijack Execution (12)	Hide Artifacts (14)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels	
			Software Deployment Tools			Hijack Execution Flow (12)		File and Directory Discovery		Data from Removable Media (3)	Non-Application (3)	
								Group Policy Discovery				
								Log Enumeration				

Unauthorized access to baby monitors

Table 1: Real-world IoT product vulnerabilities and related proposed baseline criteria

Vulnerability Factors	Example Relevant Tactics: Techniques from ATT&CK	Related Baseline Criteria
Example 1: Unauthorized Access to Baby Monitors Unauthorized individuals exploited weak authentication to access data, video cameras, and microphones in baby monitors of multiple brands. In some cases, product developers failed to respond to vulnerability reports.		
Direct access to the internet combined with weak or compromised authentication credentials leave the monitor vulnerable to unauthorized access.	• Privilege Escalation: Access Token Manipulation • Credential Access: Credentials from Password Stores • Collection: Data from Configuration Repository	Product Configuration Interface Access Control Product Education and Awareness Cybersecurity State Awareness
Internet-accessible configuration details leave the monitor and local connections (i.e., home networks) easily discoverable by adversaries.	• Collection: Data from Configuration Repository	Product Configuration Product Education and Awareness
Unencrypted sensitive data is available through the baby monitor, leaving the data vulnerable to access, modification, exfiltration, and misuse.	• Collection: Data from Information Repositories • Collection: Data from Local System	Data Protection Product Education and Awareness

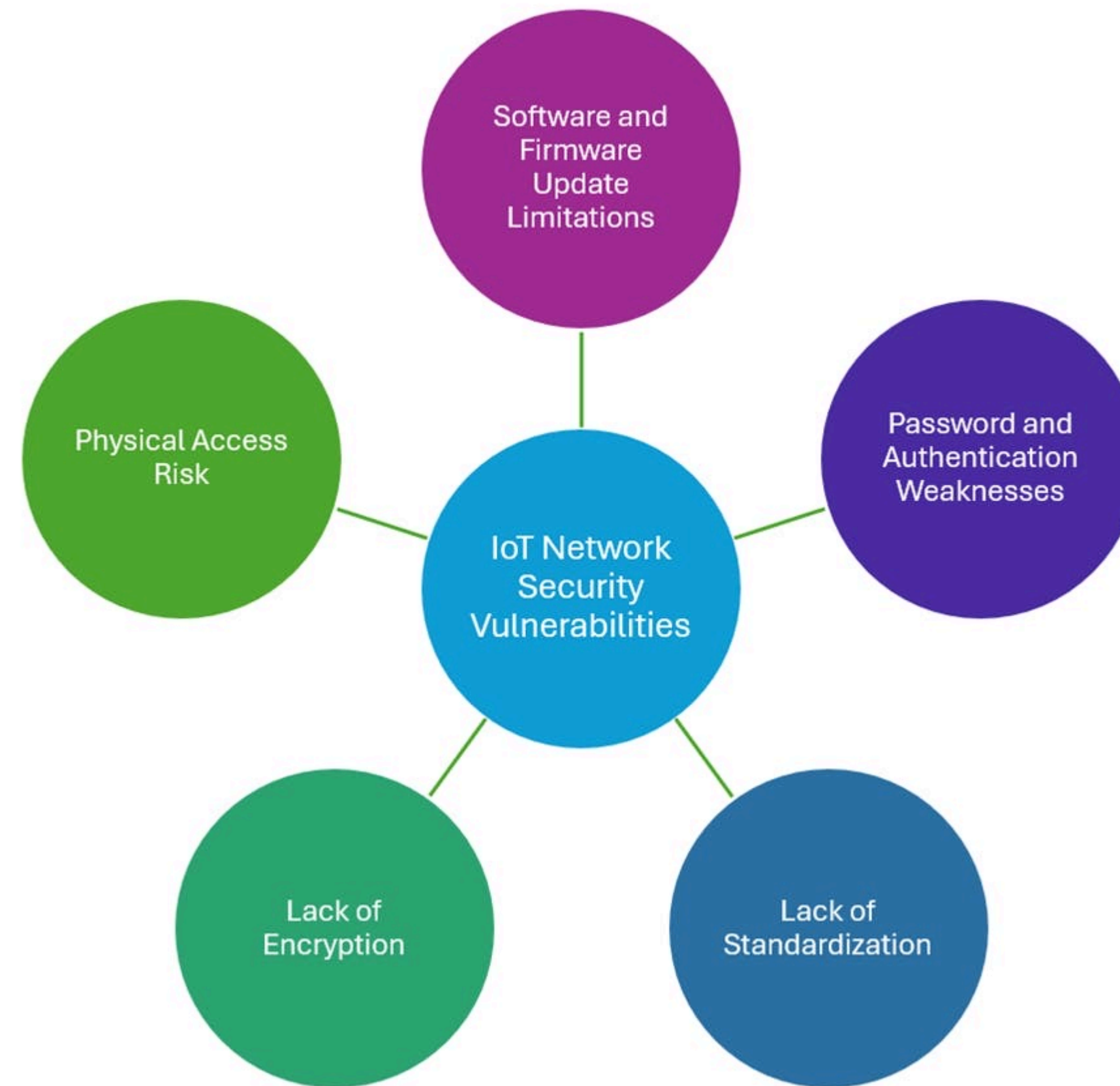
Mirai malware variants

Example 2: Mirai Malware Variants Attacks Use of weak authentication enabled the loading of malware onto the device and use of that device in Distributed Denial of Service and other attacks.		
Not using authentication, and using weak authentication credentials, leaves the IoT devices vulnerable to unauthorized access through internet and other network connections.	- Initial Access: Valid Accounts - Execution: Command and Scripting Interpreter - Privilege Escalation: Boot or Logon Initialization Scripts	Asset Identification Interface Access Control Information Dissemination Product Education and Awareness
Without intrusion detection and additional security controls for performing admin commands, the IoT device is vulnerable to having adversaries launch discovery code through the device, identify network databases, and exfiltrate the data.	- Execution: Command and Scripting Interpreter - Lateral Movement: Remote Services	Software Update Cybersecurity State Awareness Product Education and Awareness
IoT products without internal configuration and admin controls leave the products and attached networks vulnerable to having adversaries execute commands, scripts, or binaries, creating the possibility to launch malicious code or commands using the IoT product.	- Execution: Command and Scripting Interpreter - Command and Control: Data Obfuscation	Interface Access Control Documentation

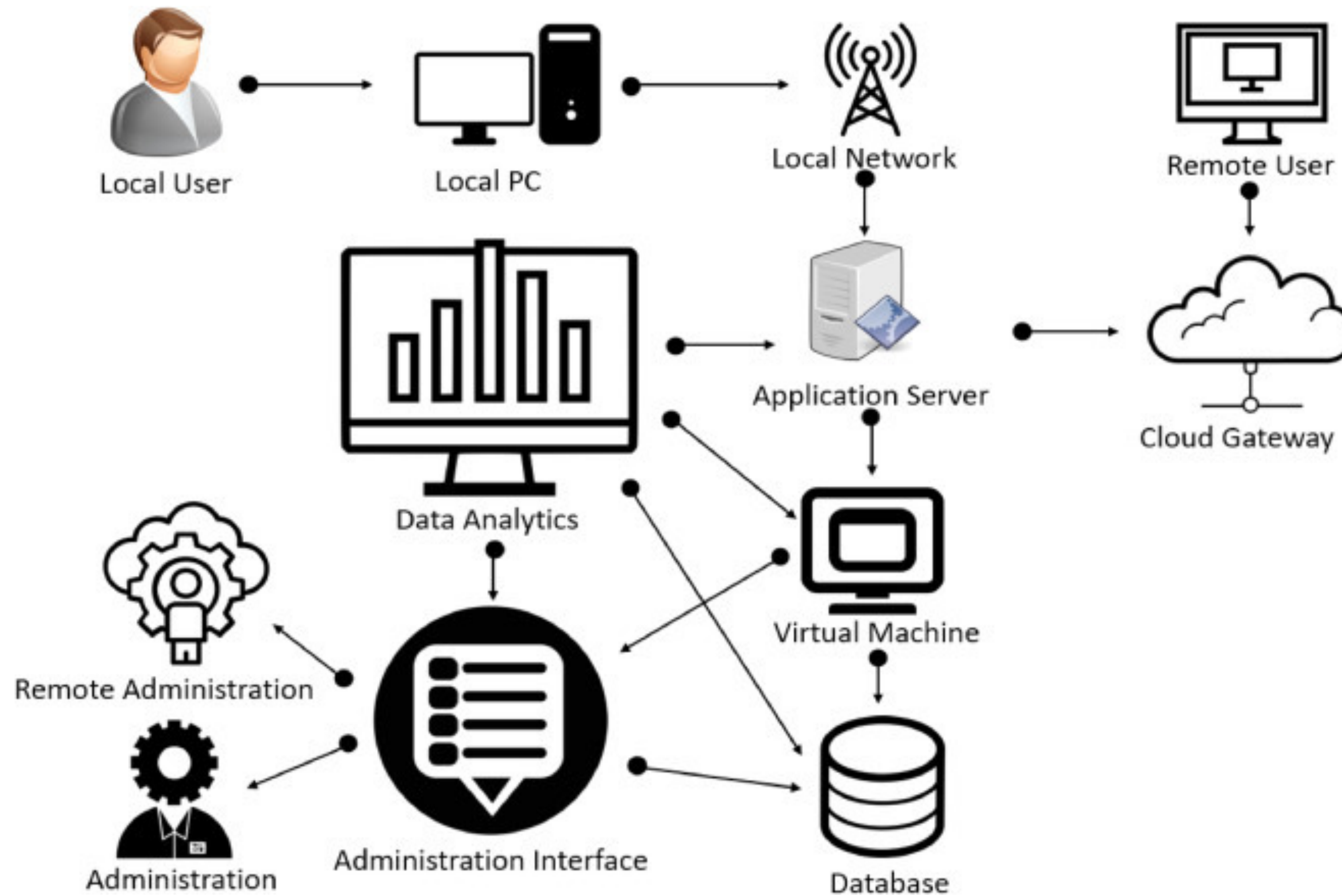
Access to data and networks through used IoT devices

Example 5: Access to Data and Networks Through Used IoT Devices Still accessible data on secondhand IoT devices putting previous owners at risk		
When data has not been removed from devices, and/or devices have not been reset to factory settings, the devices are vulnerable to having the data and device settings (which may include account credentials, sensitive images, network connection data, etc.) accessed by subsequent device owners.	• Credential Access: Credentials from Password Stores • Collection: Data from Configuration Repository - Privilege Escalation: Access Token Manipulation	Product Configuration Interface Access Control Product Education and Awareness Cybersecurity State Awareness
Devices with network configuration settings and other details enable subsequent IoT product users to gain access to associated networks.	• Collection: Data from Configuration Repository	Product Configuration Product Education and Awareness
Sensitive data in storage within used IoT products are vulnerable to access, use and misuse by subsequent users of the IoT product.	• Collection: Data from Information Repositories • Collection: Data from Local System	Data Protection Product Education and Awareness

Why is IoT security so hard?



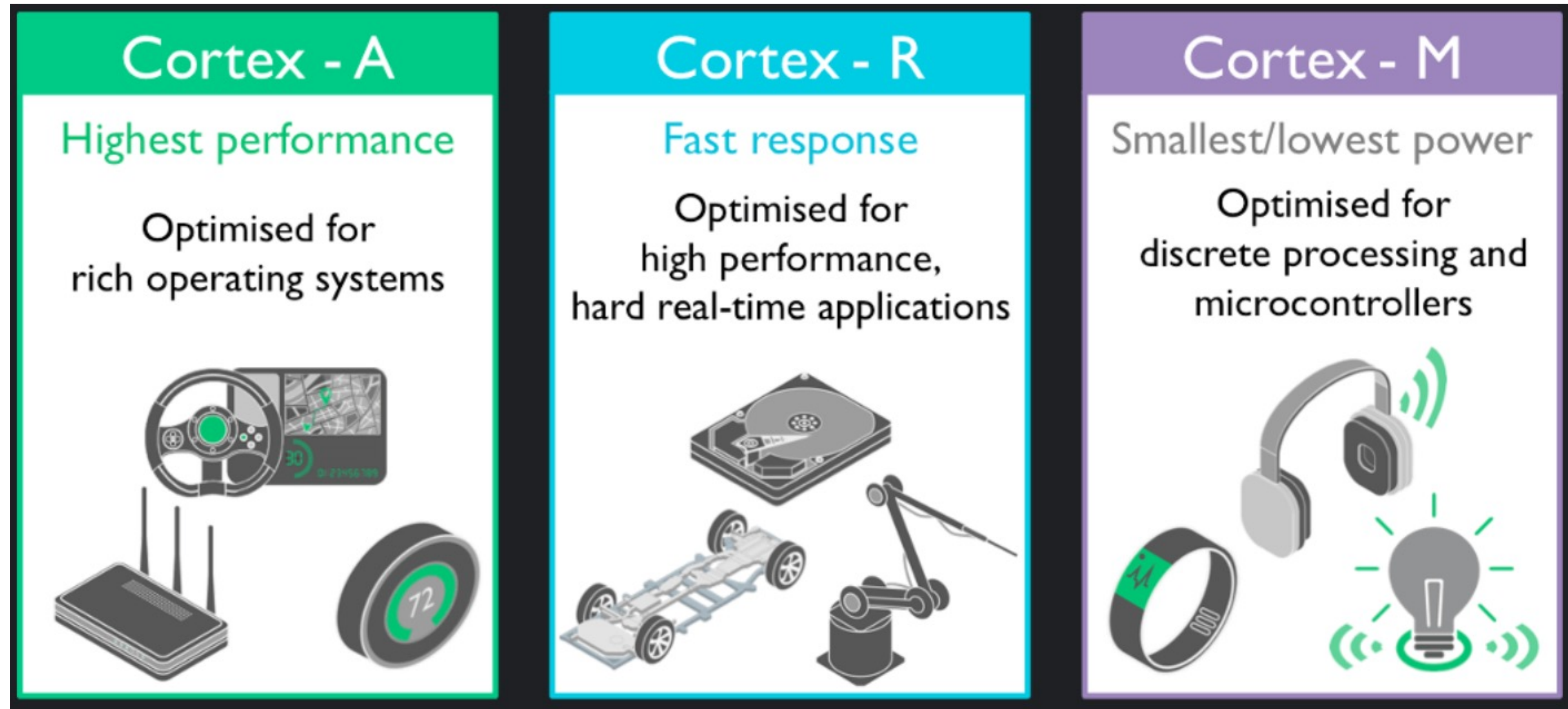
The IoT attack surface is extremely broad.



Medical devices create a separate range of difficulties.



Embedded processors have limited capabilities.



<https://developer.arm.com/community/arm-community-blogs/b/architectures-and-processors-blog/posts/introducing-cortex-a32-arm-s-smallest-lowest-power-armv8-a-processor-for-next-generation-32-bit-embedded-applications>

Devices can lose features if not supported by the manufacturer.

Dumb idea? \$1,700 “smart” bassinet loses features if you buy it used

Non-new Snoos now lose some use.

NATE ANDERSON – AUG 22, 2024 5:56 PM | 212



Even the largest tech companies strand IoT devices.

NEWS

PSA: Your Nest Thermostat may lose all smart features tomorrow

Google is pulling the plug on your smart heating



By [Jon Mundy](#)

Contributor, Tech Advisor | OCT 24, 2025 5:24 PM BST

In summary

- Support for gen 1 and 2 Nest Thermostats ends 25 October
- No more Google Home or Nest app support or software updates
- Will be limited to on-device controls for basic features

FTC: Not supporting devices may violate the law.

**FTC Staff Report:
Smart Device
Makers' Failure to
Provide Updates
May Leave You
Smarting**



FTC staff reviewed
product webpages for
184 connected products.

Nearly 89% of product
web pages failed to
disclose for how long the
manufacturer would
update the product
software.

Expert Advice on How to Protect IoT Devices

CISA's advice on how to improve the security of Internet-enabled devices:



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

[Home](#) / [News & Events](#) / [News](#) / Securing the Internet of Things (IoT)

BLOG

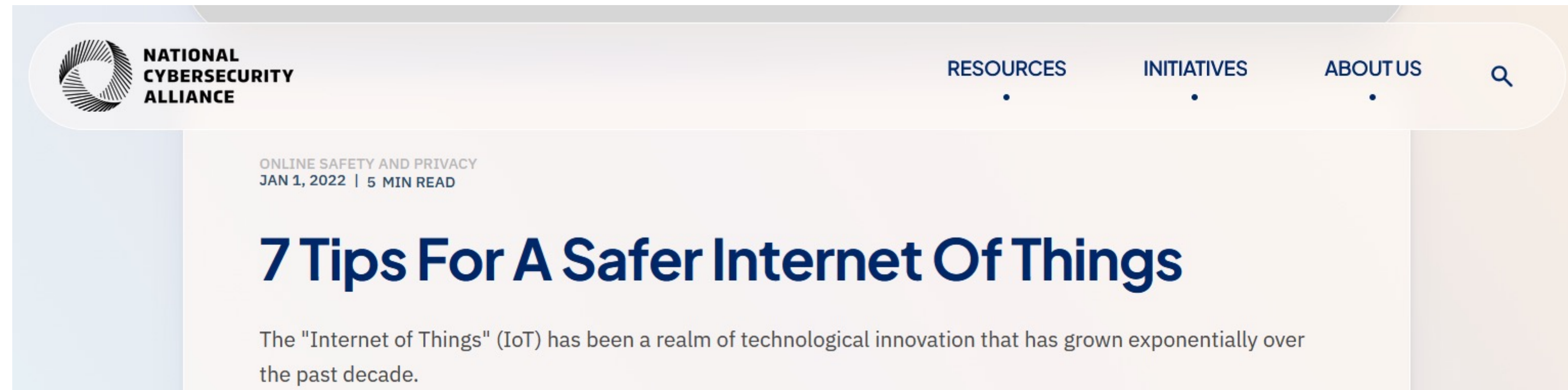
Securing the Internet of Things (IoT)

Released: February 01, 2021

- Evaluate your security settings.
- Ensure you have up-to-date software.
- Connect carefully.
- Use strong passwords.

<https://www.cisa.gov/news-events/news/securing-internet-things-iot>

National Cybersecurity Alliance advice on IoT security



- Do your homework
- Change the default passwords!
- Set privacy settings to your comfort level
- Keep them on guest network
- Stay on top of updates
- Don't use a feature? Disable it!
- Be mindful of where you place devices

Let's go to the most reliable source for good advice.

**HARVARD**
Information Security and Data Privacy

[About](#) [Policies and Standards](#) [Roles](#) [Awareness and Education](#)

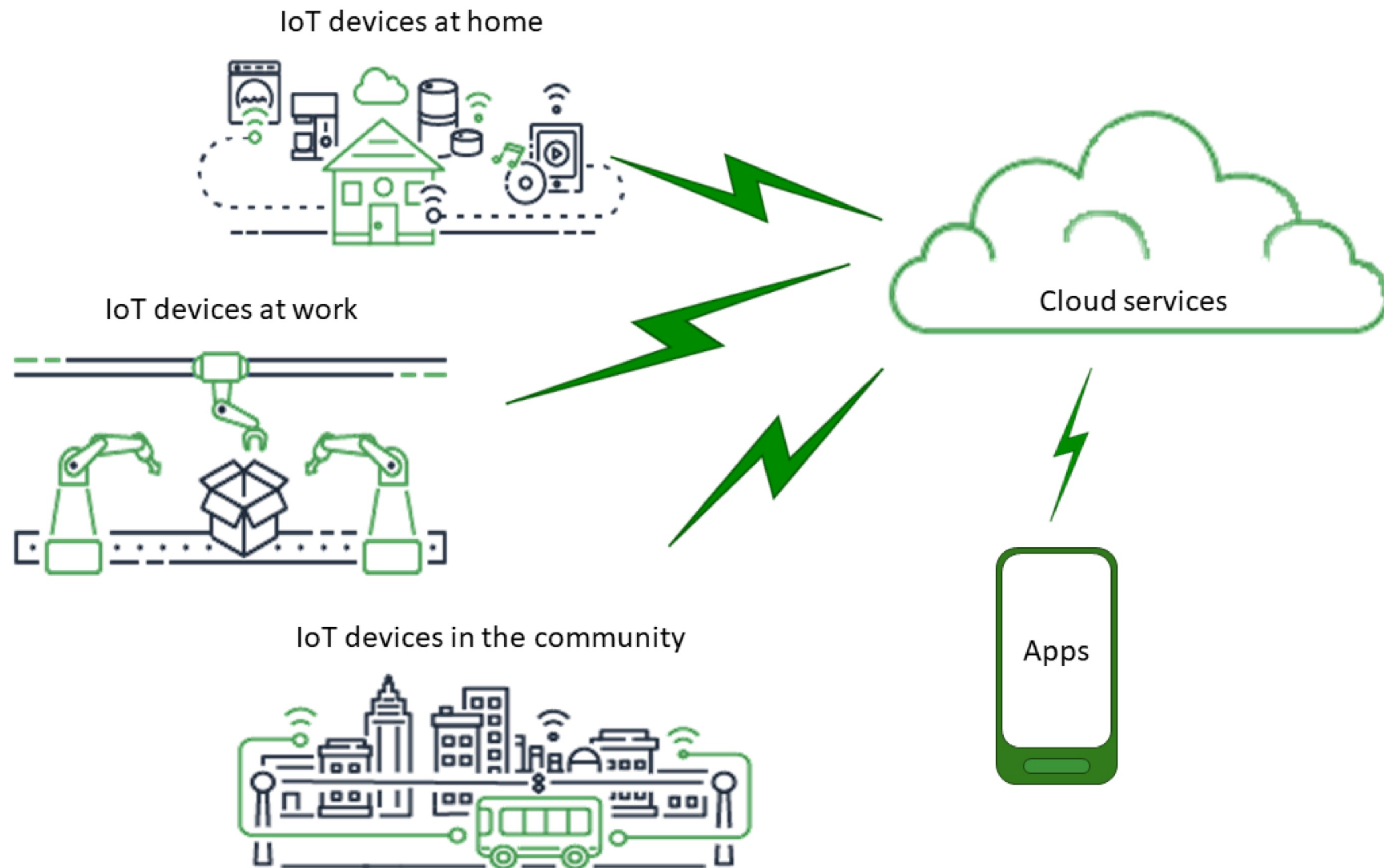
[Home](#) > [Best Practices - IoT Devices](#)

Best Practices – IoT Devices

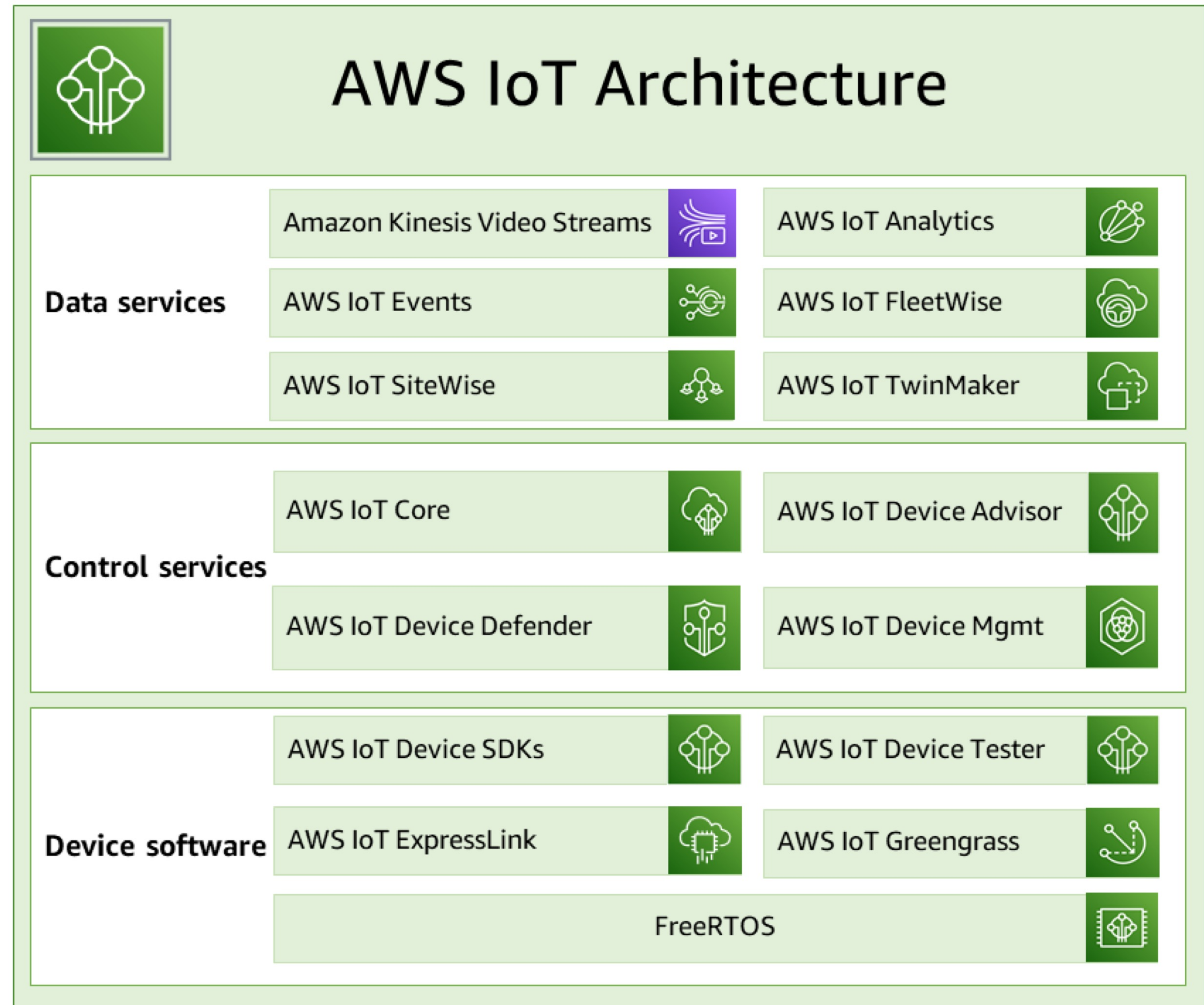
- Change Default Passwords Immediately
- Keep Your Devices Updated
- Enable Encryption
- Segment Your Network
- Purchase Devices from Reputable Vendors
- Limit Data Collection and Sharing
- Manage Remote Access Carefully
- Monitor Device Activity
- Dispose of Devices Securely
- Stay Informed

The Corporate View on How to Protect IoT Devices

AWS View of IoT

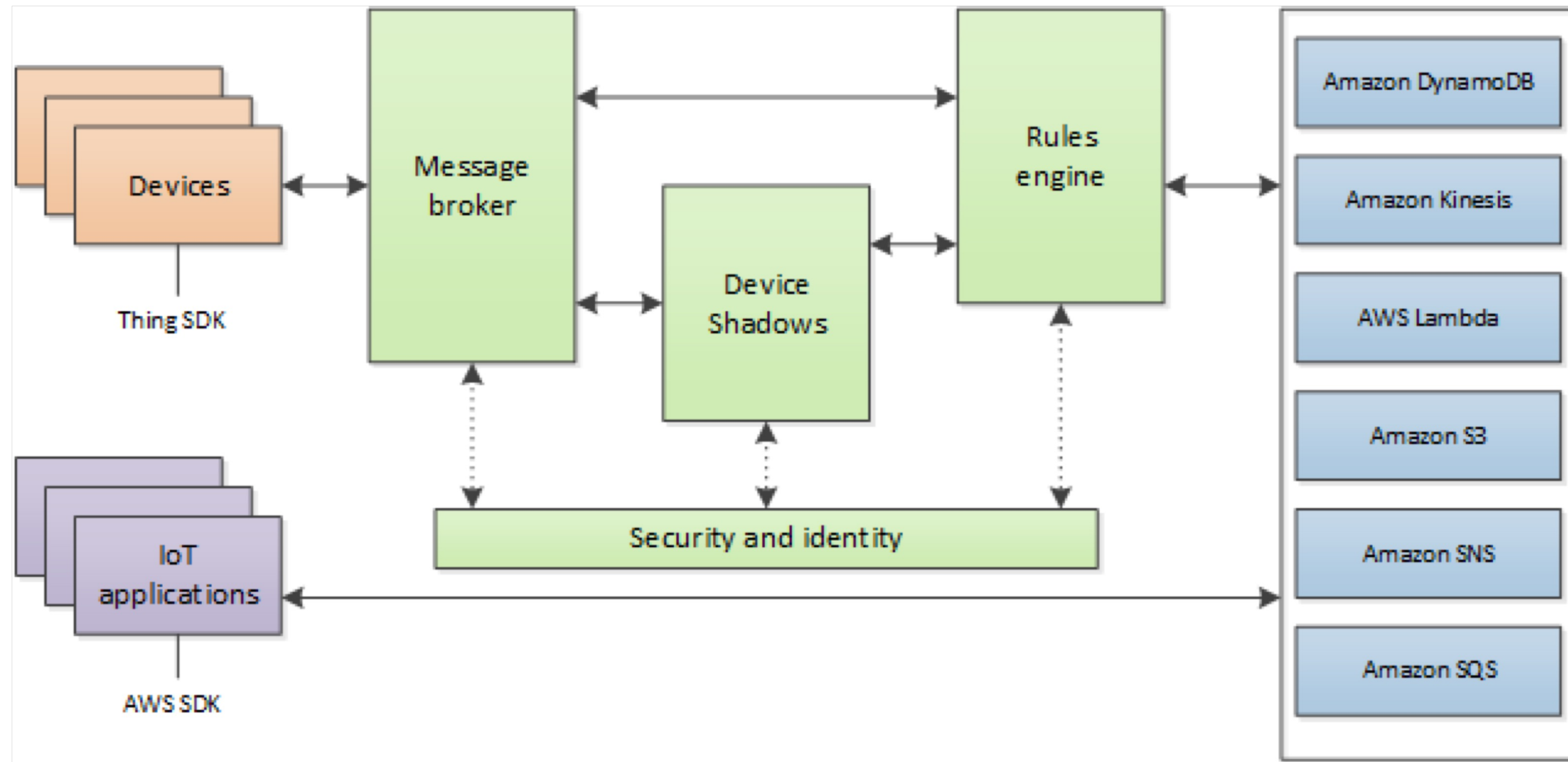


AWS tools to manage IoT

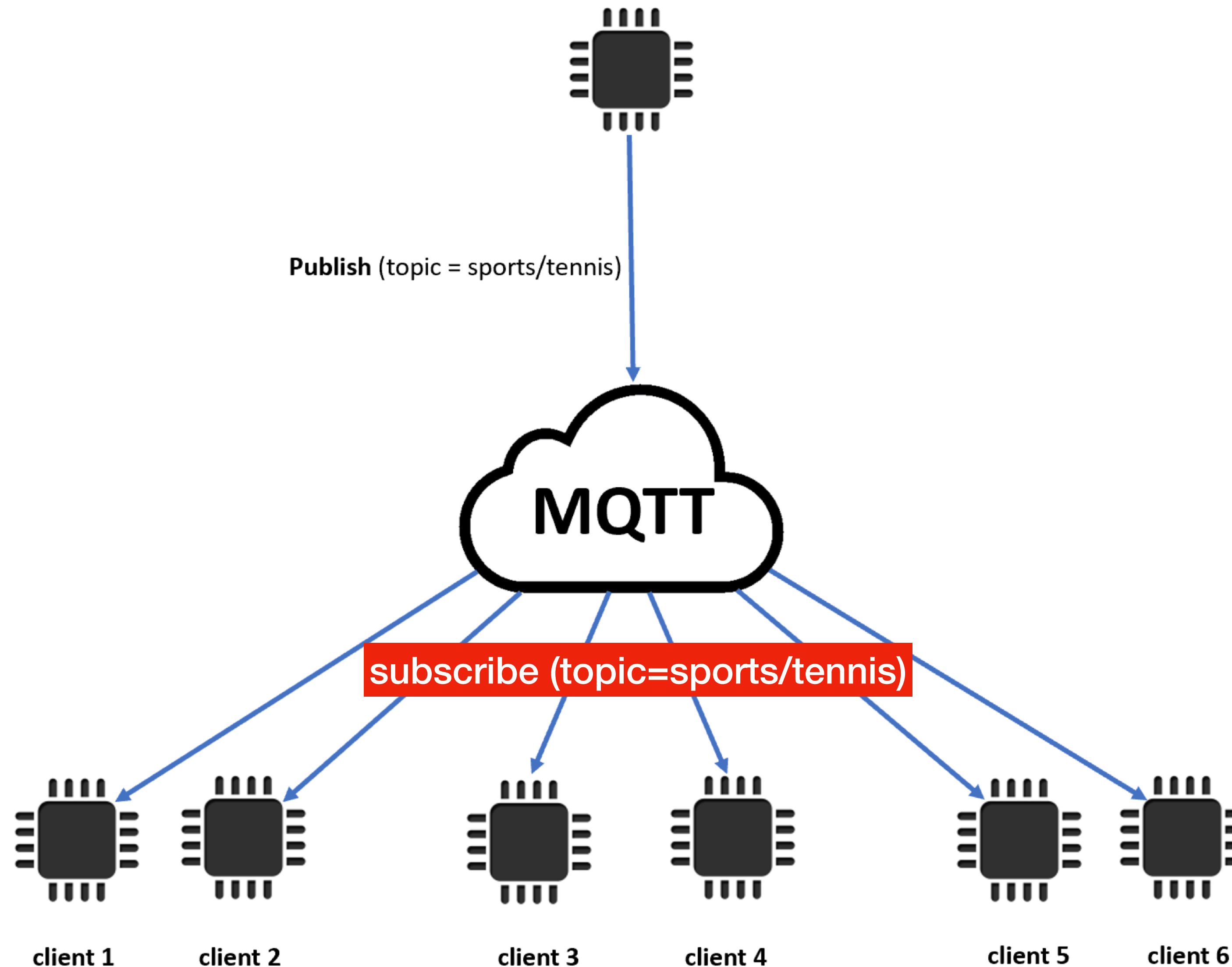


AWS IoT Core Services

AWS IoT Core provides the services that connect your IoT devices to the AWS Cloud so that other cloud services and applications can interact with your internet-connected devices.



Many IoT system use MQTT (Message Queuing Telemetry Transport) for messages.



The corporate/vendor view of IoT security.

[All Categories](#) / [IoT Security](#)

IoT Security Reviews and Ratings

What is IoT Security?

The amount of information being transmitted from things continues to rise. Much of this data originates outside of the enterprise. The scale of security risks in the Internet of Things (IoT) era is therefore much greater than in the pre-IoT environment, and the 'attack surface' is much larger. Most sensor-based things have minimal computing resources, and the opportunities for antivirus, encryption and other forms of protection within things are more restricted. Therefore, IoT security products with a variety of capabilities emerged to help dispel some of these challenges.



The Claroty Platform

By Claroty

4.9 ★★★★★ (45 Ratings)

OVERVIEW

ALTERNATIVES

Claroty provides a cyber-physical systems (CPS) protection platform to secure mission-critical infrastructure. Built on a foundation of deep industry expertise and asset visibility, the platform’s broad solution set comprises exposure management, network protection, secure access, and threat detection, and can be deployed in the cloud via Claroty xDome or on-premise with Claroty CTD. Backed by threat research from Claroty’s Team82 and a breadth of technology alliances, the Claroty Platform enables organizations to effectively reduce CPS risk with faster time-to-value and lower total cost of ownership. The company is headquartered in New York City with a presence in EMEA, Asia-Pacific, and the Americas.

Sector-specific security vendors



CyberMDX Healthcare Cybersecurity

By Forescout (CyberMDX)

5 ★★★★★ (15 Ratings)

OVERVIEW

ALTERNATIVES

CyberMDX is an enterprise that specializes in IoT security with a unique focus on safeguarding global health delivery systems. The company offers cloud-based cyber security solutions aimed at bolstering the burgeoning Internet of Medical Things. With the primary role of identifying endpoints and assessing vulnerabilities, CyberMDX strives to detect, respond to, and counter cyber incidents effectively. To support compatibility and ease of use, the solution developed by CyberMDX is notably agentless, scalable, and designed for seamless integration into existing infrastructures. The company also provides insights into emerging trends, technologies, and management techniques shaping the sphere of healthcare administration.

Show Less

Show Less Details ^

Ratings Breakdown

5 Stars		93%
4 Stars		7%
3 Stars		0%
2 Stars		0%
1 Star		0%

From Our Reviewers

- “Navigating CyberMDX's Unique Medical Device Cybersecurity Capabilities”
- “An effective tool to track, manage and secure your Clinical Assets & BioMeds”
- “CyberMDX - Great Product with Excellent Insight to IoMT.”

[Read All Reviews](#)

Asset Management



Armis Centrix

By Armis
5 ★★★★★ (7 Ratings)

OVERVIEW ALTERNATIVES

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization’s cyber risk exposure in real time. In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, protect and manage all critical assets. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7. Armis is a privately held company headquartered in California.

Show Less

Show Less Details ^

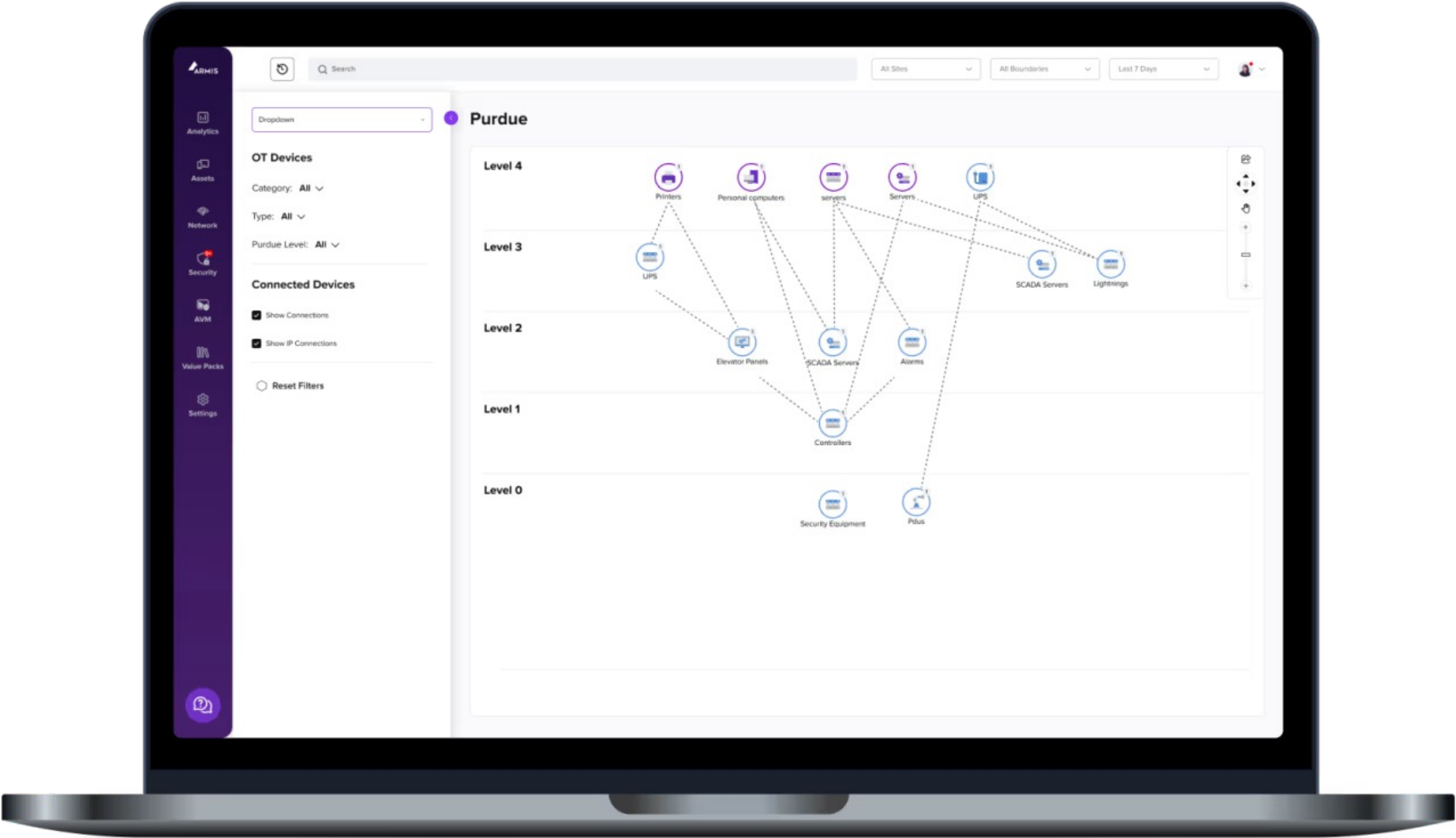
Ratings Breakdown

5 Stars	86%
4 Stars	14%
3 Stars	0%
2 Stars	0%
1 Star	0%

From Our Reviewers

- “Armis helped me sleep better at night”
- “Armis provides us the map of all our assets and networks”
- “Great visibility”

[Read All Reviews](#)



OT/ IoT Security: Keeping Critical Infrastructure Safe and Secure 24/7

Armis Centrix™ for OT/IoT Security delivers comprehensive protection for critical infrastructure and industrial environments. With the freedom to choose an **on-premises** and/or SaaS deployment option, Armis delivers the cyber exposure management you seek, along with the operational resilience you demand. Seamlessly integrating with existing security architectures, it enhances resilience, streamlines compliance, and ensures real-time ICS management at scale.

Every IoT device needs a cert



DigiCert IoT Trust Manager

By DigiCert
4.6 ★★★★★ (19 Ratings)

OVERVIEW ALTERNATIVES

DigiCert is a digital trust provider that serves for various enterprises worldwide. The company focuses on ensuring secured online engagements for individuals, businesses, governments, and consortia, handling their digital footprints.

Show Less Details ^

Ratings Breakdown

5 Stars		53%
4 Stars		42%
3 Stars		0%
2 Stars		5%
1 Star		0%

From Our Reviewers

- “Navigating Complexity: A Look at New IoT Certificate Management”
- “Securing Data Exchanges: The Strengths of IoT Security”
- “DigiCert IoT Trust Manager Exceeds Expectations with Reliability & Scalability”

[Read All Reviews](#)



Entrust Certificate Services

By Entrust
4.5 ★★★★★ (8 Ratings)

OVERVIEW ALTERNATIVES

Entrust's focus lies in promoting secure interactions in the digital world by providing solutions for identity verification, payment security and digital infrastructure.

The company offers a broad range of critical services that facilitate trust in multi-cloud environments, mobile identity, hybrid work, machine identity, electronic signatures, encryption and more.

Its solutions help advance Zero Trust journeys with access management and authorization tools and to secure multi-cloud operations by protecting and managing keys, secrets, and certificates, all while preparing for a post-Quantum future.

Entrust also secures digital interactions such as account opening and onboarding, enabling users with unified digital credentials and digital signing.

Finally, it provides instant and central issuance solutions that allow banks, governments, and enterprises to issue trusted digital and physical credentials.

Entrust has customers across over 150 countries and over 2,800 employees.

Show Less

Show More Details v

Router Security

March 2026: FCC bans all foreign-made consumer routers



NEWS FROM THE FEDERAL COMMUNICATIONS COMMISSION

FACT SHEET: FCC Updates Covered List to Include Foreign-Made Consumer Routers, Prohibiting Approval of New Models

Update Follows Determination by Executive Branch Agencies that Consumer-Grade Routers Produced in Foreign Countries Threaten National Security

WASHINGTON, March 23, 2026—Today, the Federal Communications Commission [updated](#) its [Covered List](#) to include all consumer-grade routers produced in foreign countries. Routers are the boxes in every home that connect computers, phones, and smart devices to the internet. This followed a [determination](#) by a White House-convened Executive Branch interagency body with appropriate national security expertise that such routers “pose unacceptable risks to the national security of the United States or the safety and security of United States persons.”

Key points...

National Security Determination on the Threat Posed by Routers Produced by Foreign Countries

March 20, 2026

<https://www.fcc.gov/sites/default/files/NSD-Routers0326.pdf>

- “Compromised routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses’ networks.”
- “a majority of the routers in American homes and businesses are produced outside the United States.”
- “Recently, malicious state and non-state sponsored cyber attackers have increasingly leveraged the vulnerabilities in small and home office routers produced abroad to carry out direct attacks against American civilians in their homes.”
- “Additionally, routers produced abroad were directly implicated in the Volt, Flax, and Salt Typhoon cyberattacks which targeted critical American communications, energy, transportation, and water infrastructure.”

FCC bans on imports require a determination of unacceptable risk to national security.

National Security Determination on the Threat Posed by Routers Produced by Foreign Countries

March 20, 2026

Summary of Determination:

The President's 2025 National Security Strategy (NSS) says, "the United States must never be dependent on any outside power for core components—from raw materials to parts to finished products—necessary to the nation's defense or economy. We must re-secure our own independent and reliable access to the goods we need to defend ourselves and preserve our way of life."¹ One of these core components that is necessary to both our nation's defense and economy is routers. Routers are the key networking device that enable American homes, schools, businesses, critical infrastructure providers, and emergency services to connect to the internet every day. A majority of the routers currently in Americans' homes and businesses are manufactured in foreign countries.² Given the criticality of routers to the successful functioning of our nation's economy and defense, the United States can no longer depend on foreign nations for router manufacturing.

Why focus on routers?



World ▾ Business ▾ Markets ▾ Sustainability ▾ Legal ▾ Breakingviews ▾ More ▾

Hundreds of thousands of US internet routers destroyed in newly discovered 2023 hack

By Christopher Bing

May 30, 2024 4:34 PM EDT · Updated a year ago

🔖

Aa

🔗



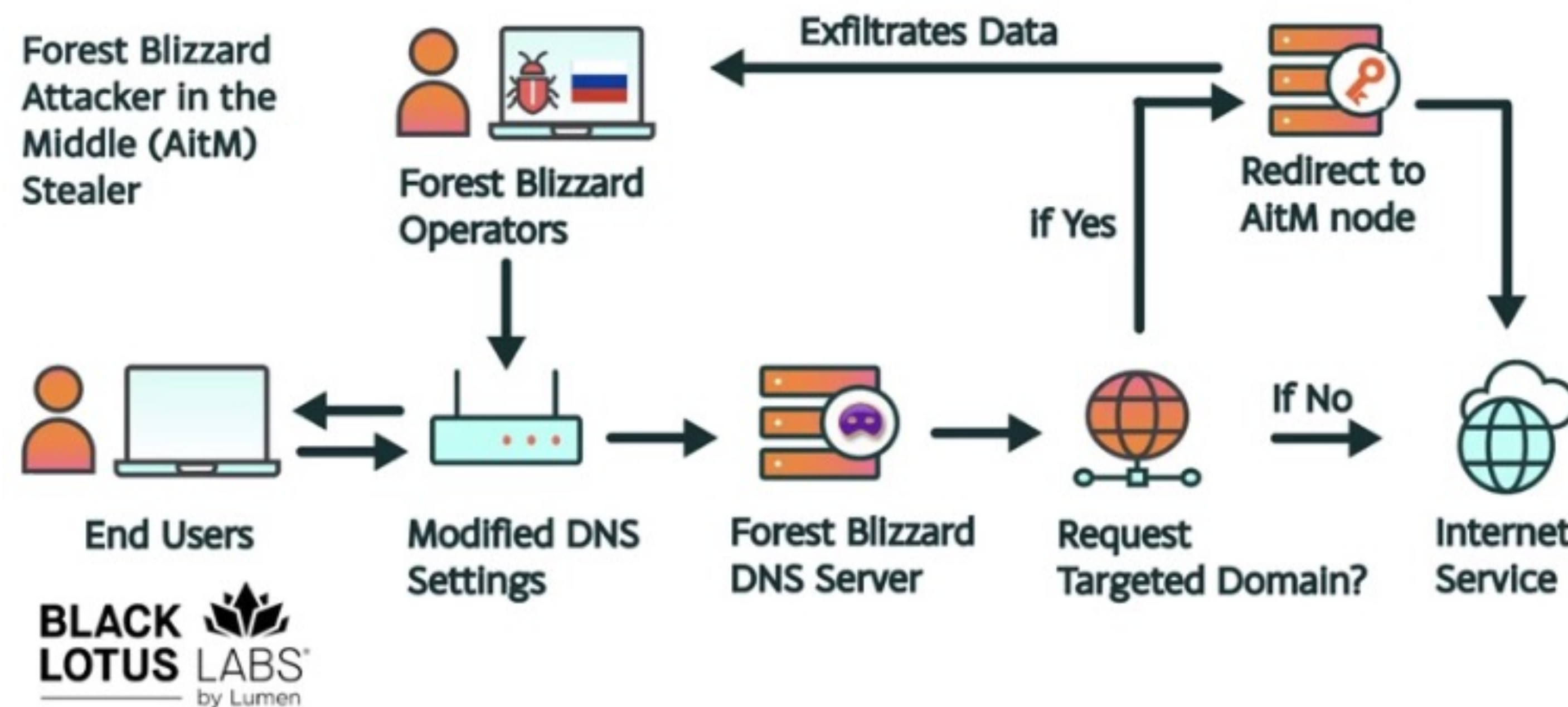
A projection of cyber code on a hooded man is pictured in this illustration picture taken on May 13, 2017. REUTERS/Kacper Pempel/Illustration//File Photo [Purchase Licensing Rights](#) 

Russia hacked older routers.

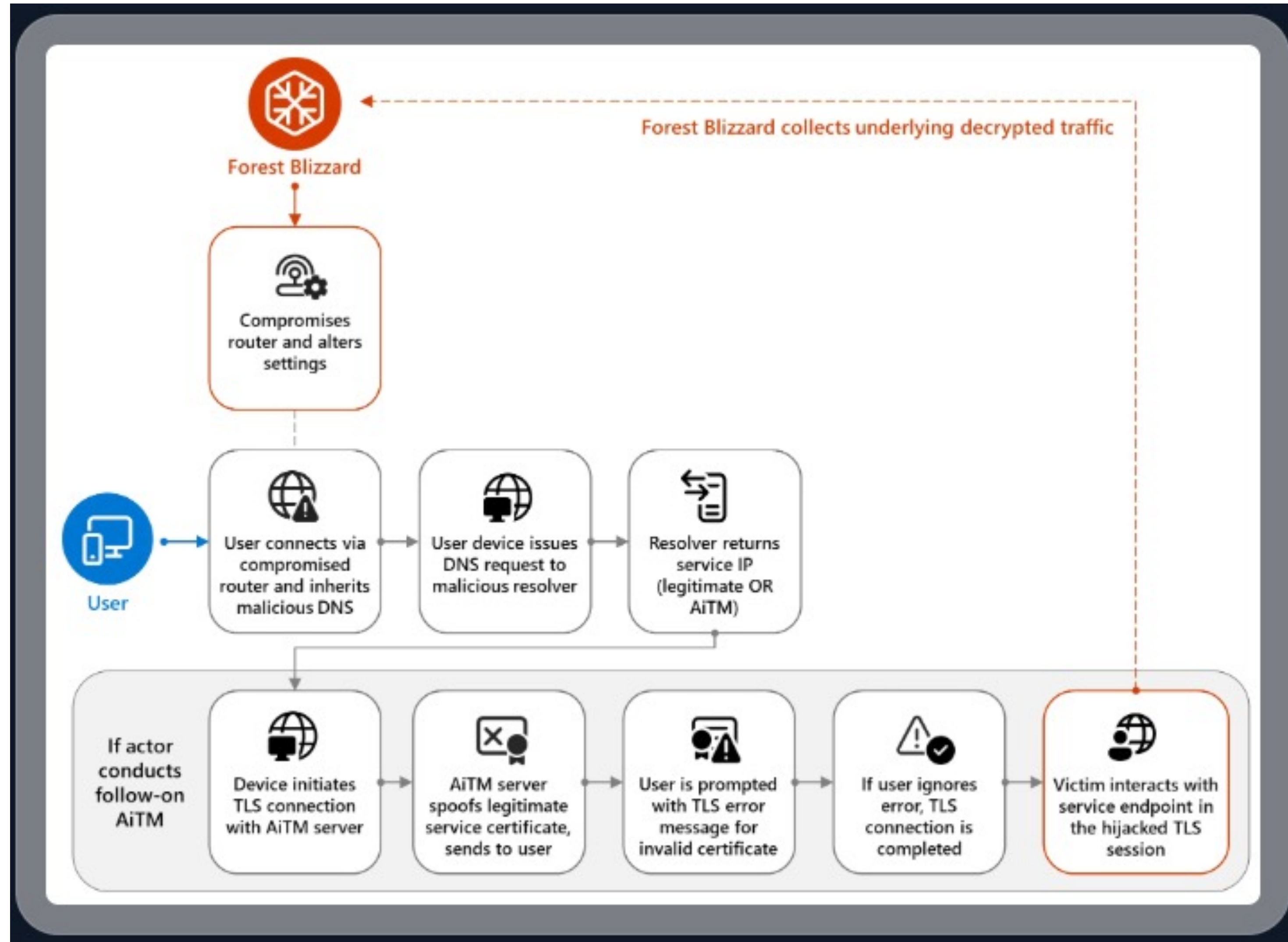
Russia Hacked Routers to Steal Microsoft Office Tokens

April 7, 2026

22 Comments



Forest Blizzard redirected DNS to hostile sites.



NIST published guidance on consumer router security in 2024.

NIST Internal Report NIST IR 8425A

Recommended Cybersecurity Requirements for Consumer-Grade Router Products

Michael Fagan
Katerina Megas
Paul Watrobski
Jeffrey Marron
Barbara Cuthill
*Applied Cybersecurity Division
Information Technology Lab*

David Lemire
Brad Hoehn
Chris Evans
Hill

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8425A>

September 2024



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

A.6.15. Software Update 1

Each consumer-grade router product component can receive, verify, and apply verified software updates that are signed and firmware updates that are signed and may be encrypted.

Related Standards Requirements:

BBF GEN.OPS.22, GEN.OPS.23

CL KEY-004, KEY-005, SB-001, SU-001, SU-005, SBOM-009, SB-002, SU-003

BSI (4.2)

IMDA 4.3

SP 800-193 4.1.1(4), 4.1.2(1-4), 4.2.1.1, 4.2.1.2(1), 4.2.4(3, 5), 4.3.1(2), 4.4.1(2-6)

All software update packages should be signed by the source of the update (e.g., manufacturer), but when applicable (e.g., when routers are leased from ISPs) other entities may also cryptographically sign updates, adding another layer of security.

A.6.16. Software Update 2

The consumer-grade router product implements measures to keep software (including firmware) on router product components up to date (i.e., automatic application of updates or consistent customer notification of available updates via router components), including provisions to prevent firmware rollback attacks (e.g., not allowing the rollback of firmware to a version with known vulnerabilities).

Related Standards Requirements:

BBF GEN.OPS.19, GEN.OPS.20, MGMT.LOCAL.15, MGMT.LOCAL.21, MGMT.LOCAL.22

CL SB-003, SU-002, SU-006, SBOM-003, SBOM-007, SBOM-008, SBOM-010

BSI (4.1.2), (4.2)

IMDA 4.3

SP 800-193 4.1.2(5), 4.2.1.3, 4.4.1(1, 10, 11, 13)

The NIST IoT Labeling Project

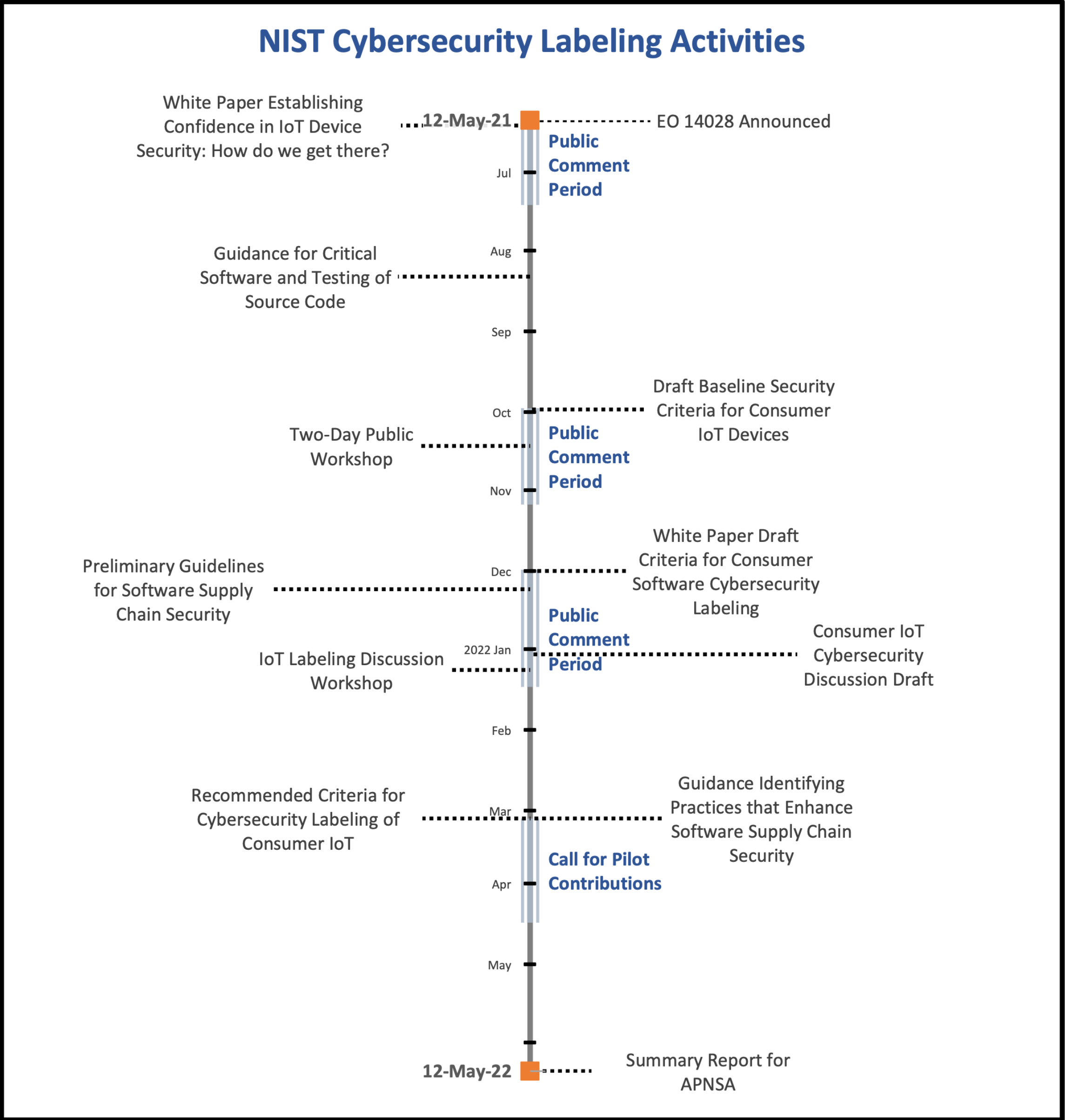
In 2022, NIST released a report on cybersecurity labeling for consumer IoT devices.

**Report for the Assistant to the President for National Security Affairs (APNSA) on
Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software**

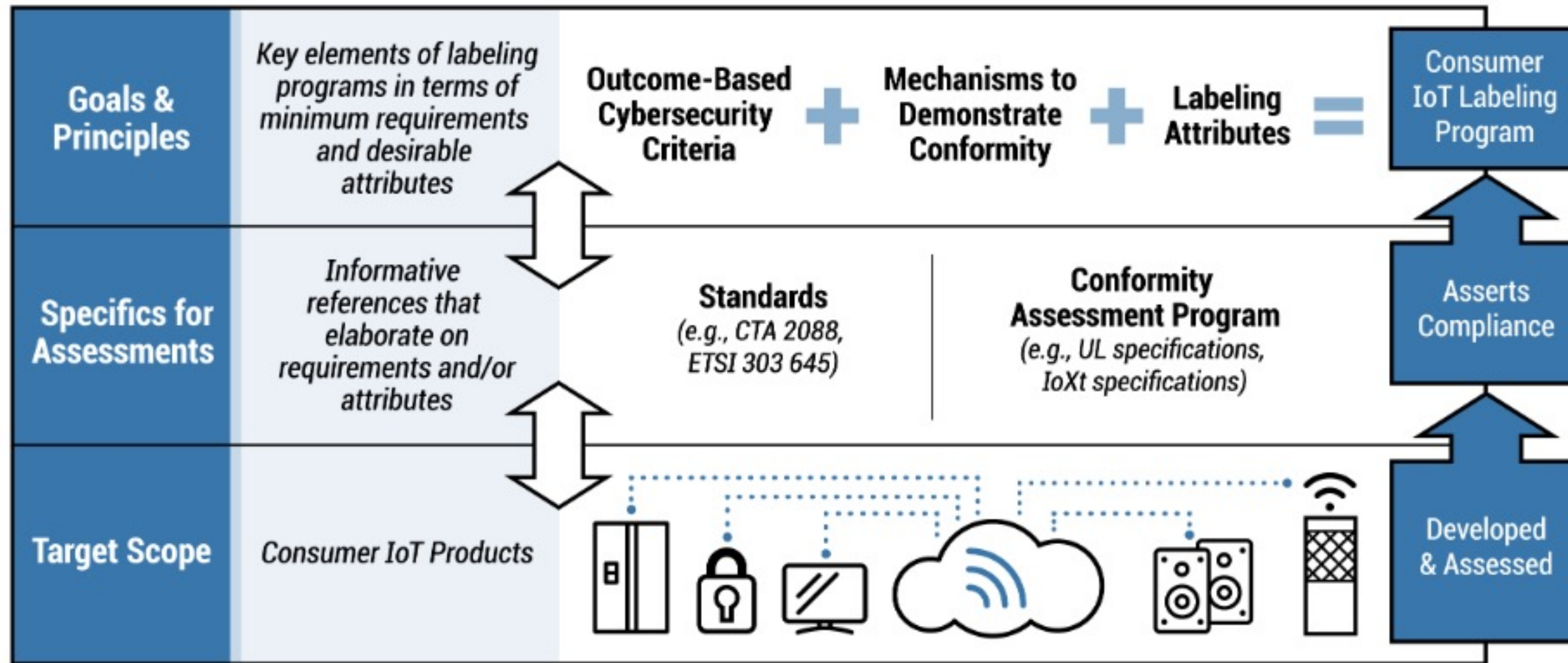
*A summary review of labeling actions called for by Executive Order (EO) 14028: Improving the
Nation's Cybersecurity*

May 10, 2022

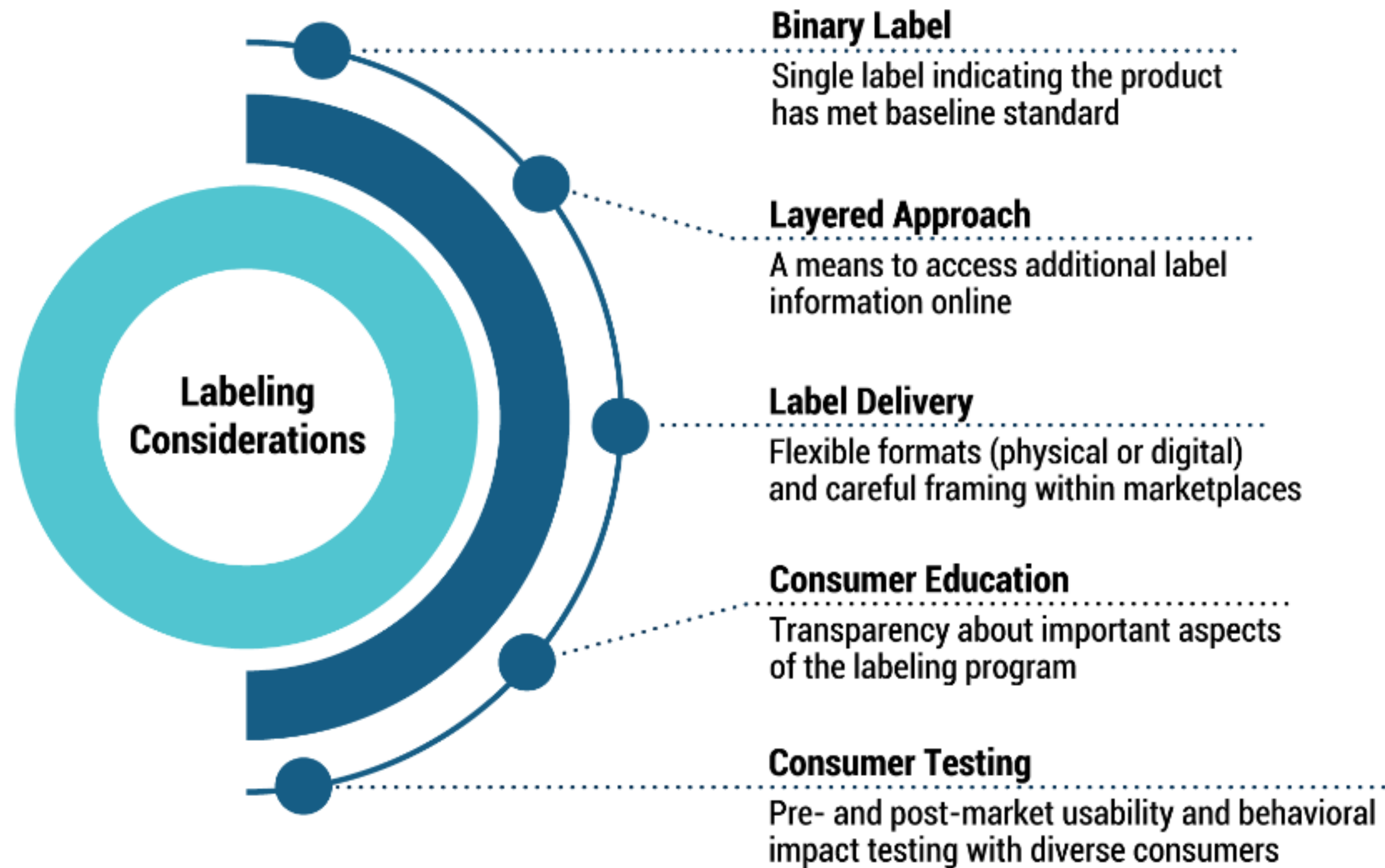
The report was the endpoint of a process started by executive order.



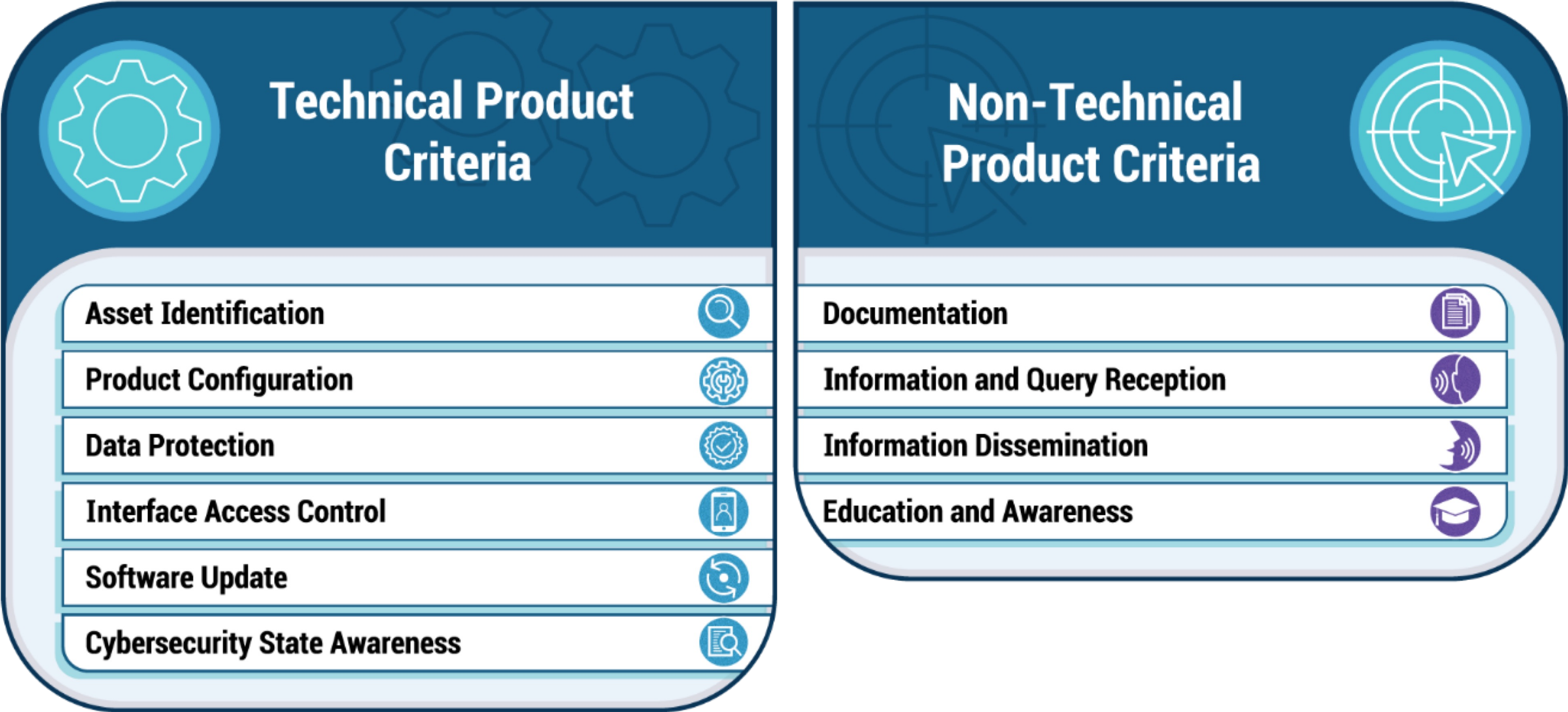
NIST labeling project



NIST labeling considerations



NIST labeling project: Product Criteria



Baseline IoT Product Criteria

NIST labeling project Claims

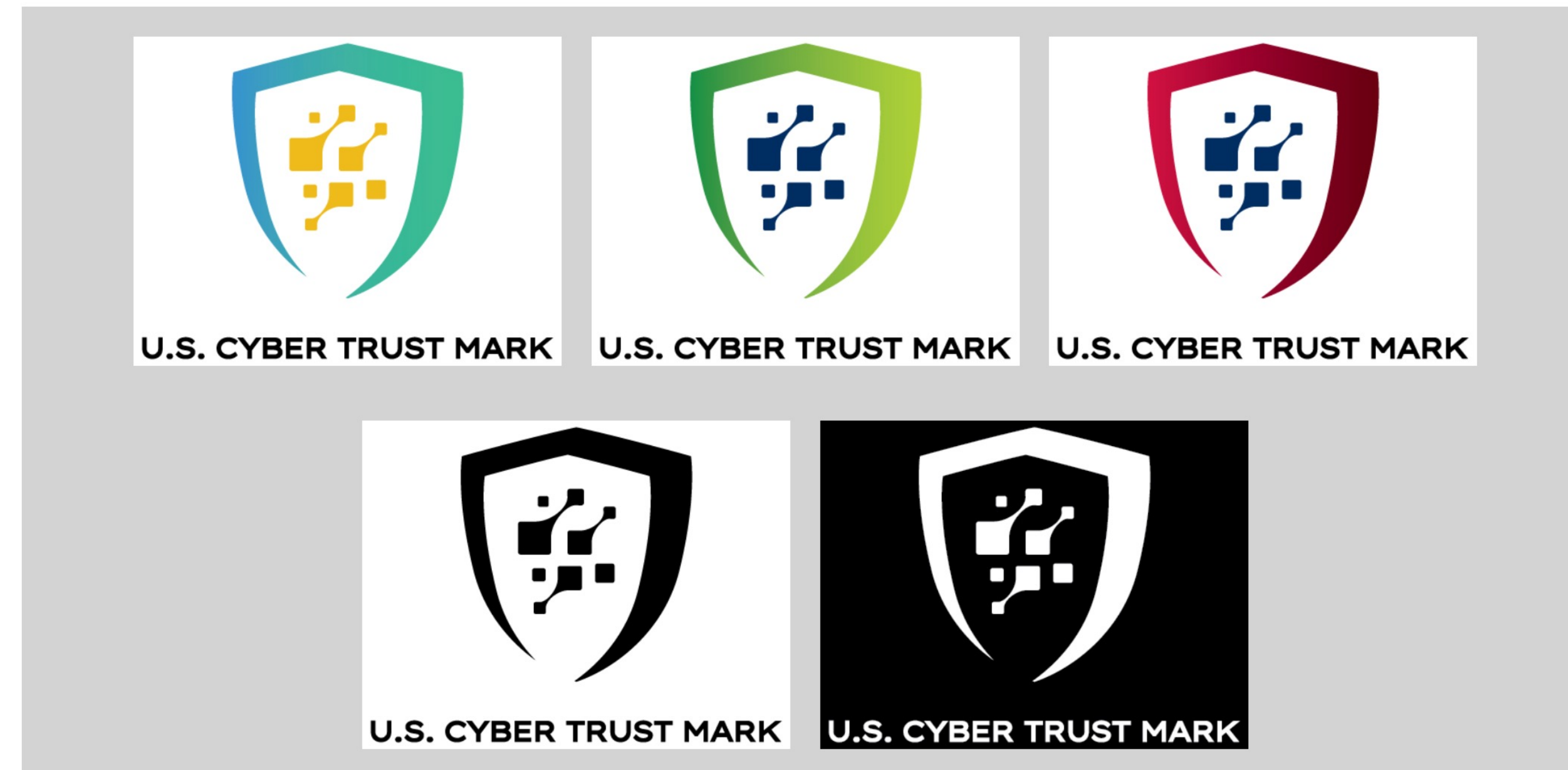
Descriptive Claims	Secure Software Development Claims
Claimant	Implements a Secure Development Process
Label Scope	Practices Secure Design and Vulnerability Remediation
Label-Software Link	Practices Responsible Vulnerability Disclosure
Claim Date	Provides for Software Integrity and Provenance
Security Update Status	Uses Multifactor Authentication (if applicable)
Minimum Duration of Security Update Support	Free from Hard-Coded Secrets
Security Update Method	Uses Strong Cryptography
	User Data is Identified and Secured

Consumer Software Technical Baseline Criteria

2024: FCC voted to create a labeling program.

Certification Mark – U.S. Cybersecurity Labeling Program for Smart Devices

This is the proposed U.S. Cyber Trust Mark logo, for which the FCC is seeking registration as a certification mark from the U.S. Patent and Trademark Office. This logo has been developed in conjunction with the FCC's proposed cybersecurity labeling program. See [Fact Sheet and Notice of Proposed Rulemaking](#). The logo may not be used without the prior express written consent of the FCC. Anyone educating consumers about the mark or the proposed labeling program (including members of the media) may contact MediaRelations@fcc.gov for permission to use the logo in the context of such efforts.



Next week's reading: Light Commands



Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems

Takeshi Sugawara, *The University of Electro-Communications*; Benjamin Cyr, Sara Rampazzi, Daniel Genkin, and Kevin Fu, *University of Michigan*

<https://www.usenix.org/conference/usenixsecurity20/presentation/sugawara>

This paper is included in the Proceedings of the
29th USENIX Security Symposium.

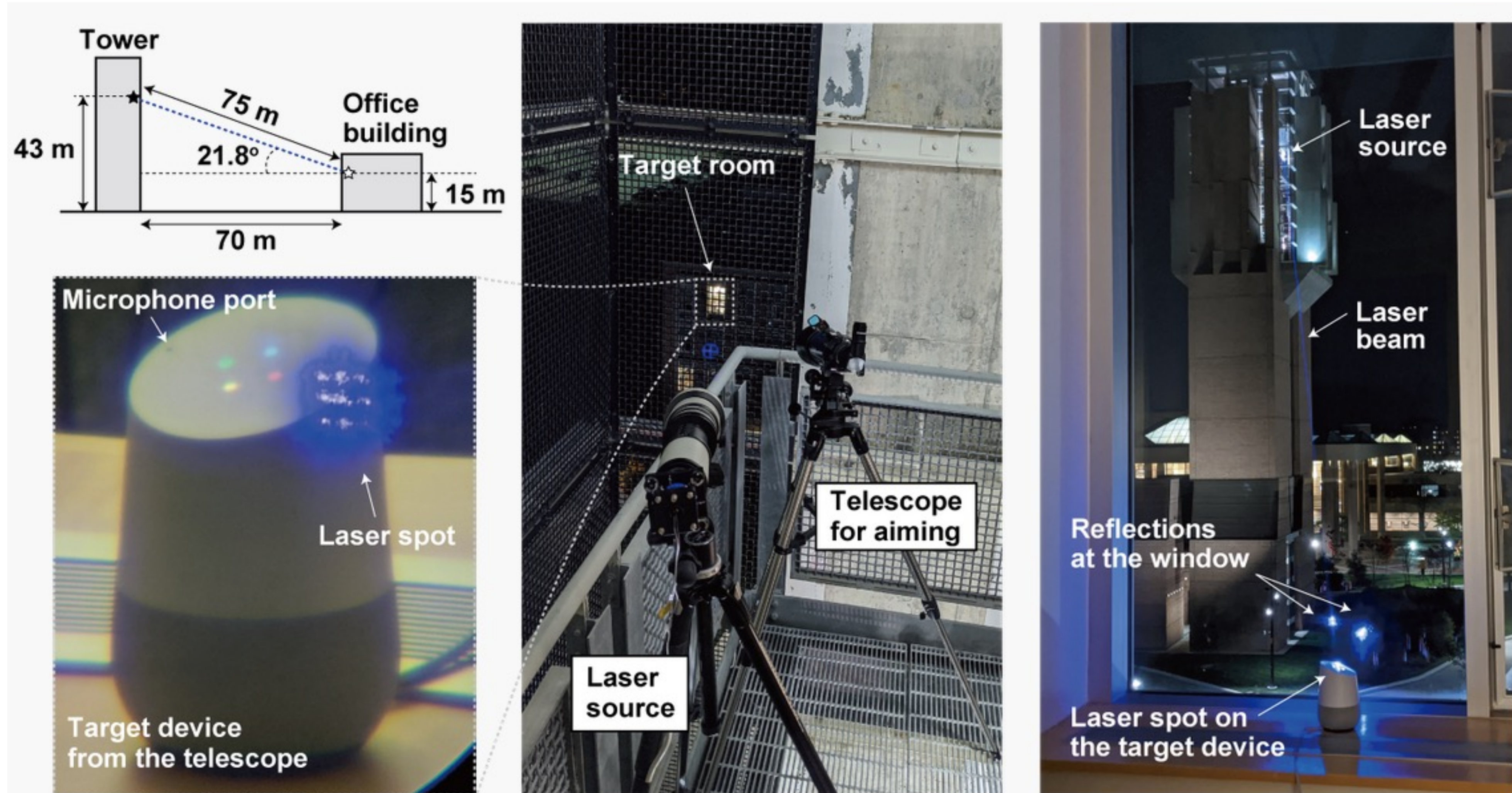
August 12–14, 2020

978-1-939133-17-5

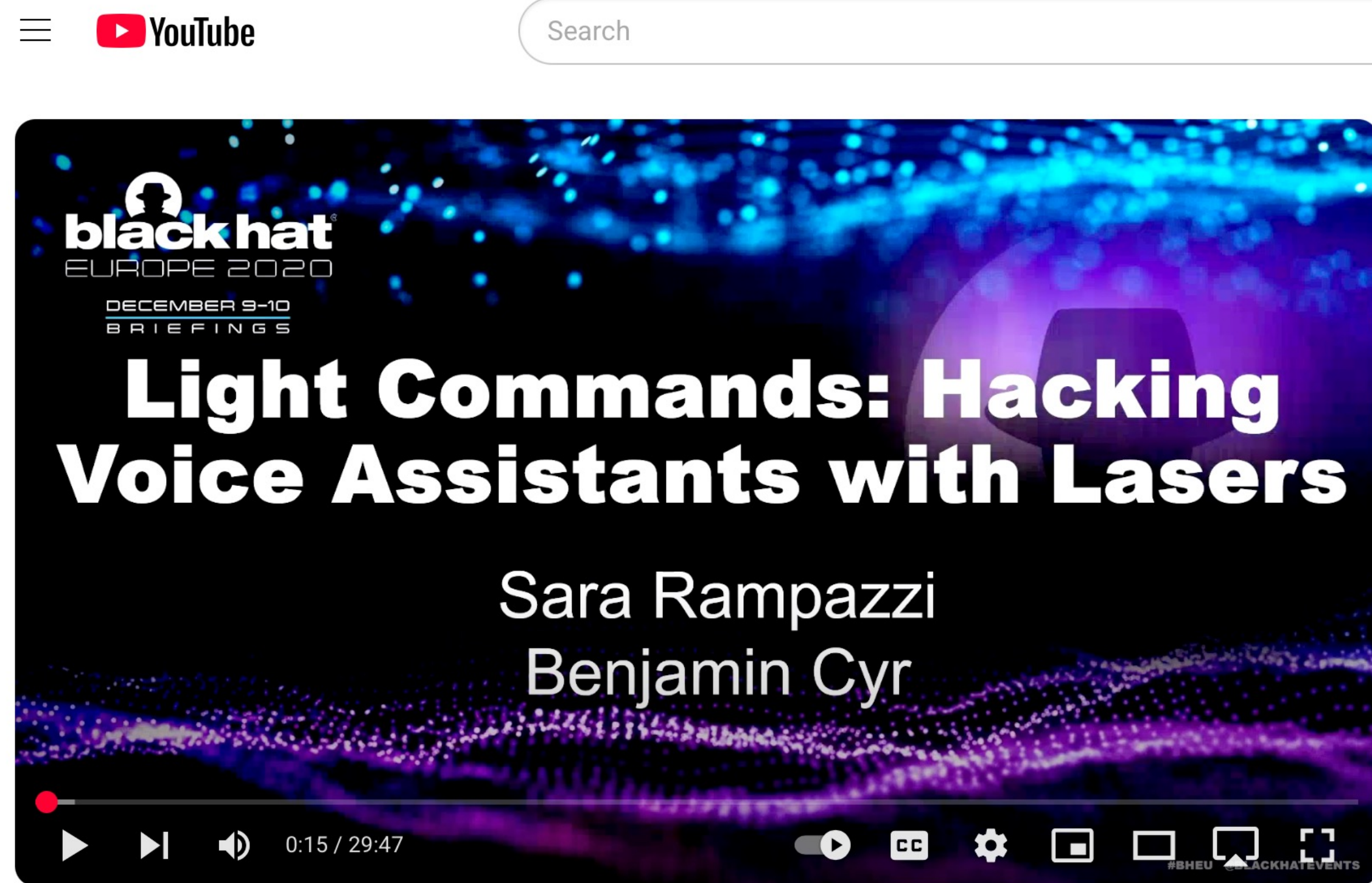


Open access to the Proceedings of the
29th USENIX Security Symposium
is sponsored by USENIX.

Using lasers to attack voice control systems (e.g., Amazon Echo/Alexa)



Visit the website: <https://lightcommands.com>
Watch the videos!



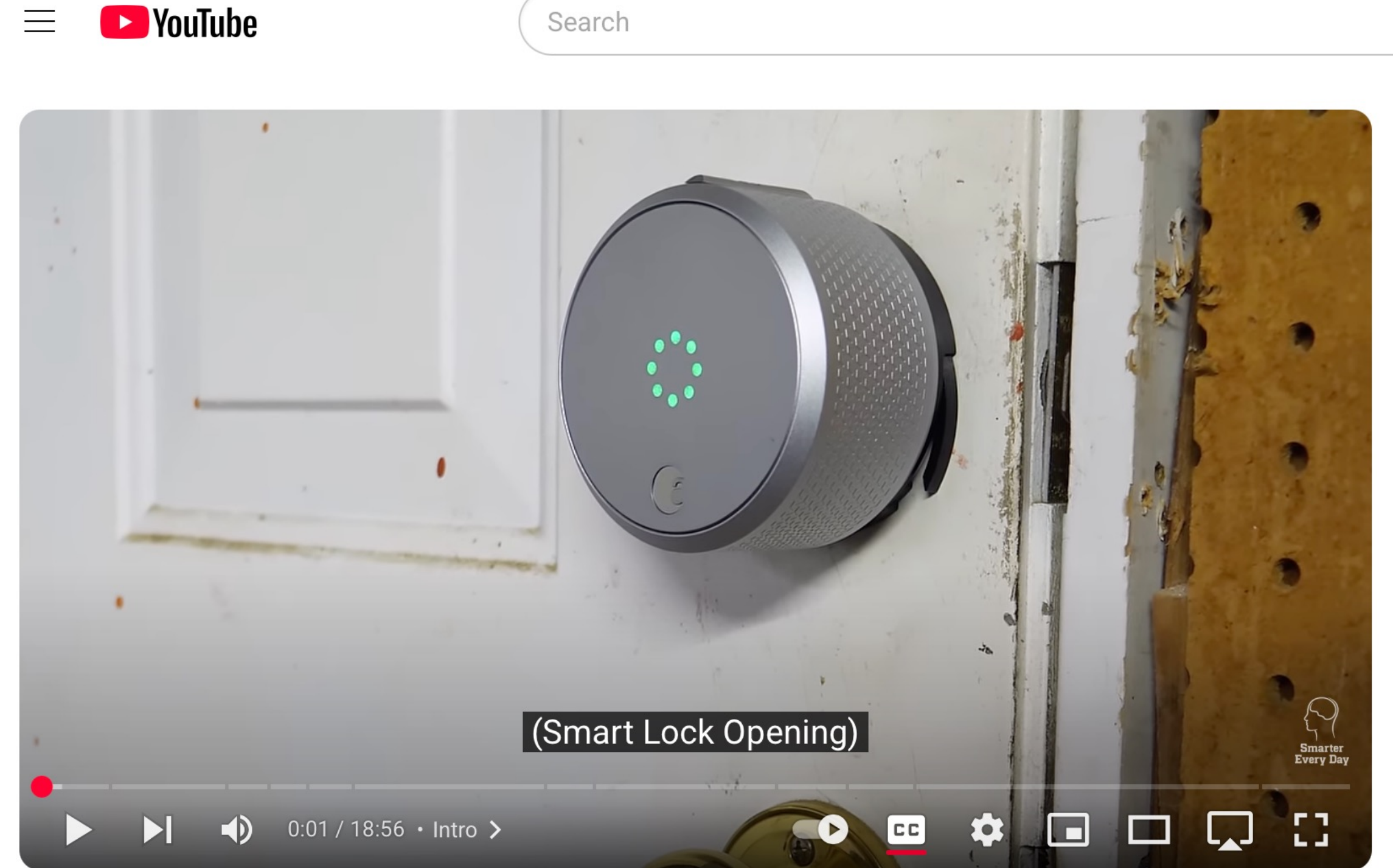
Light Commands: Hacking Voice Assistants with Lasers

 **Black Hat** 244K subscribers [Subscribe](#) [36](#) [Share](#) [Save](#) [...](#)

1.4K views 3 years ago

In the near future, our homes will employ potentially dozens of IoT devices. These devices listen to our voice commands using sophisticated microphones. Our laser-based injection attack Light Commands shows how microphones can respond to light as if it was sound... ..more

<https://www.youtube.com/watch?v=L3CAZWLoG1Y>



Breaking Into a Smart Home With A Laser - Smarter Every Day 229

 **SmarterEveryDay** 11.7M subscribers [Subscribe](#) [197K](#) [Share](#) [Save](#) [...](#)

4.8M views 5 years ago

If you feel like this has earned your support on Patreon please consider clicking here: [/ smartereveryday](#)
Note 12/28/19: The lock company notified me that they've updated their software to lock the user out after 4 incorrect attempts to enter a PIN. ...more

<https://www.youtube.com/watch?v=ozIKwGt38LQ>

For next week

- Read Sugawara
 - Comment and respond on Perusall
 - Watch the presentation video (optional but cool!)
 - Take the Reading Quiz on Canvas
- Participate in Ed Board discussion
 - Reply with suggestions for topics for Class 15
- Finish Lab 7 (due April 27)