Securing the Hyperconnected World

Andy Young
November 2, 2022

Abstract

Through wearables, AR, and connected healthcare devices become ubiquitous, people are increasingly reliant on nonstop, secure connectivity for health, information, and entertainment. With this great convenience comes great risk; some threats are obvious and some quite subtle. In this discussion, we'll examine the three key links in the chain, potential weaknesses and how to secure them:

- Endpoint devices themselves
- The communication network, increasingly 5G
- Back-end cloud services

As these are often provided by different entities, standards and interoperability become important, but each of these links is subject to risks and limitations imposed by the other. In this presentation, we'll discuss the best practices for secure design and validation at each step to ensure a trusted and reliable hyper-connected world.

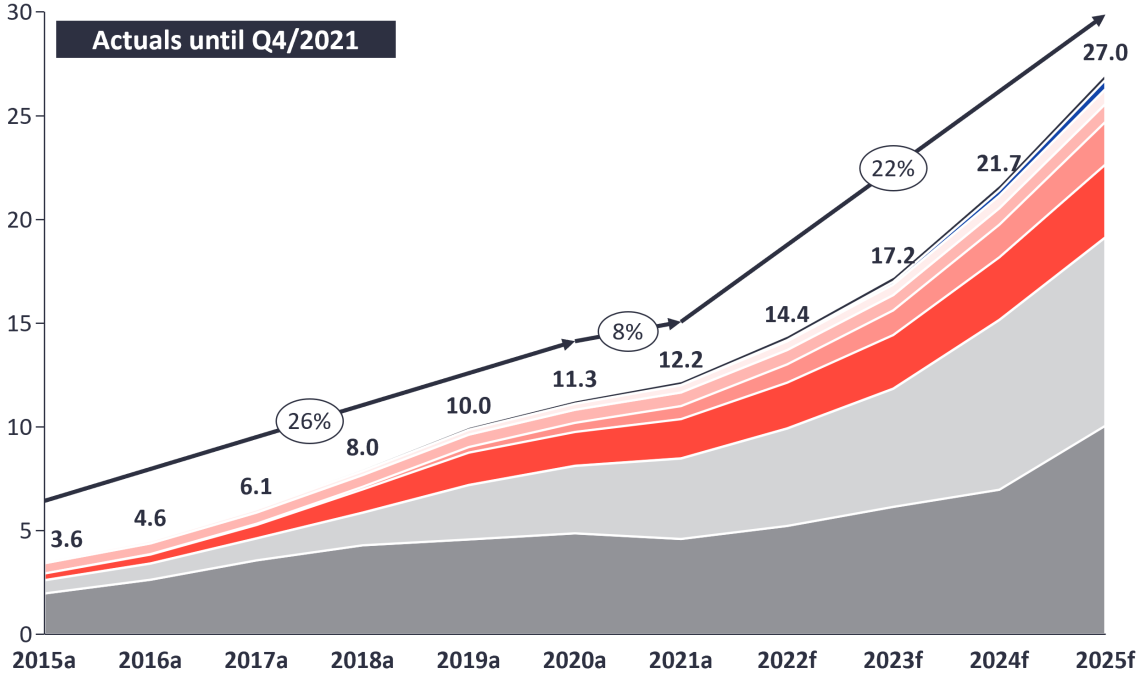
IOT ANALYTICS

May 2022

Your Global IoT Market Research Partner

Global IoT Market Forecast [in billion connected IoT devices]

Number of global active IoT Connections (installed base) in Bn



CONNECTIVITY TYPE	CAGR 20-21	CAGR 21-25
Wireless Neighborhood Area Networks (WNAN)	17%	11%
5G IoT	-	159%
Other	22%	20%
Wired IoT	4%	7%
LPWA	42%	34%
Legacy Cellular (2G/3G/4G)	16%	17%
Wireless Local Area Networks (WLAN)	19%	24%
Wireless Personal Area Networks (WPAN)	-6%	22%

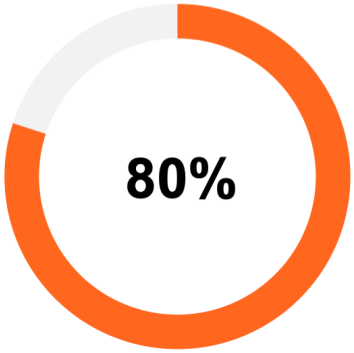
XX% = CAGR

Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh, such as Wi-SUN; Other includes satellite and unclassified proprietary networks with any range.

Source: IoT Analytics Research 2022.

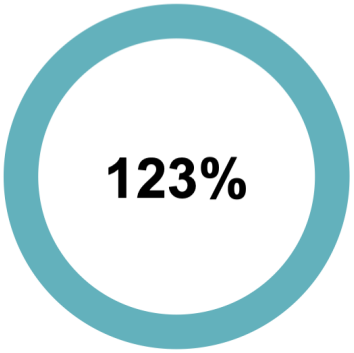
https://iot-analytics.com/number-connected-iot-devices/

IOT Attacks On The Rise



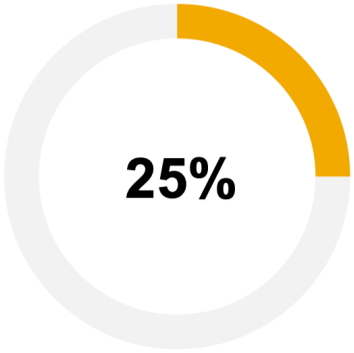
Healthcare Organizations

Faced an IOT security incident in the previous 18 months



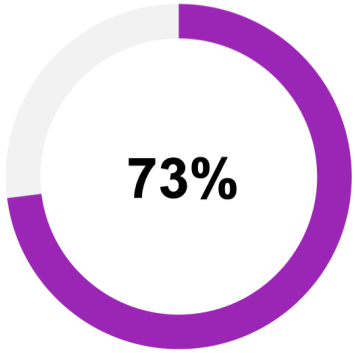
IOT Attacks in Healthcare

Yearly increase in IoT malware attack volume in healthcare



Industrial Control Systems

Increase in ICS vulnerability disclosures in 2nd half of 2021



IV Pumps Vulnerable

Most IV pumps have a serious cybersecurity vulnerability

Supply Chain

Most manufacturers use off-the-shelf communication chipsets from **established vendors**

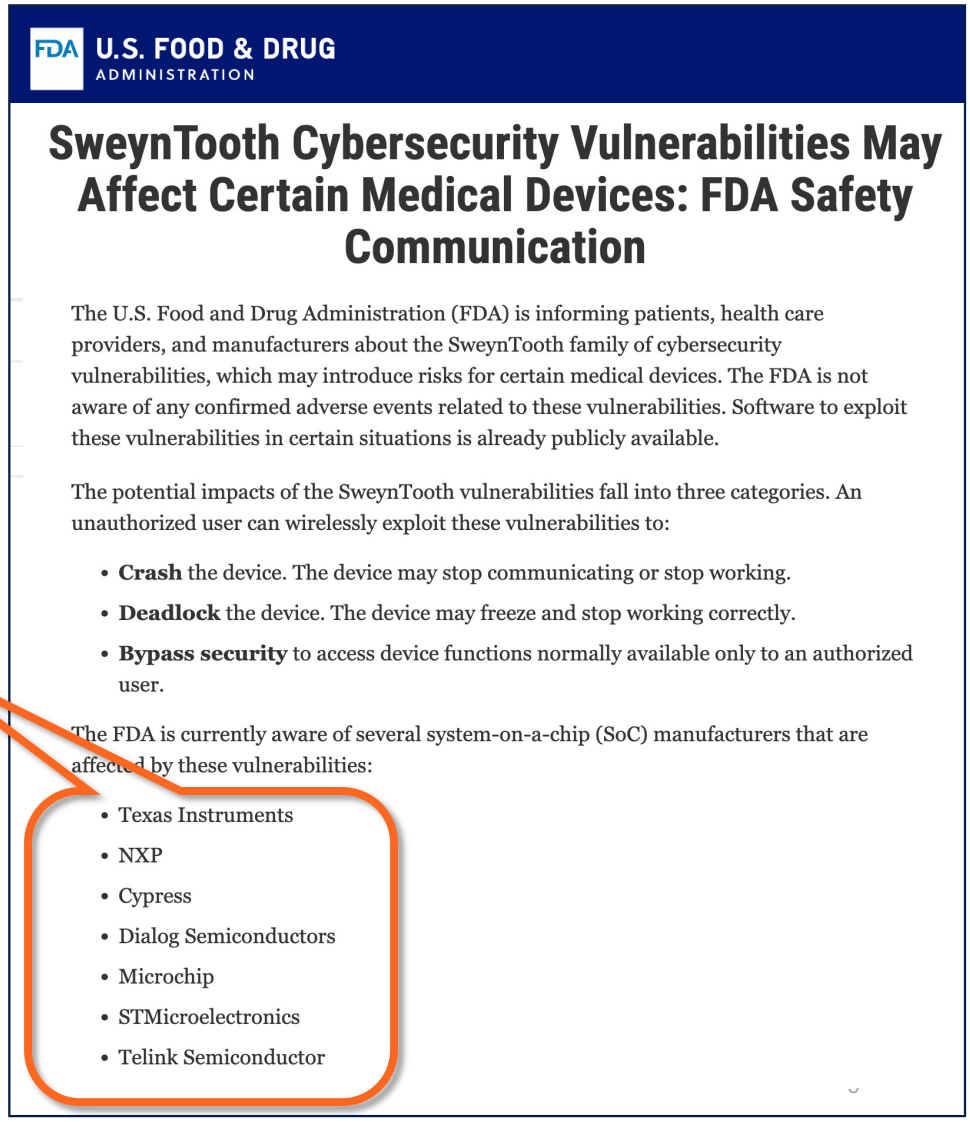
Those chipsets **may not be fully tested** or have latest firmware

When critical vulnerabilities are discovered, device **manufacturers must scramble** to address flaws and rush updates

Brand damage, **expensive recalls**, compliance risk

Result of **inadequate testing**

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

Video Doorbell

The WiFi video stream from a popular video doorbell can be disabled with a Bluetooth Low Energy attack by anyone within radio range.

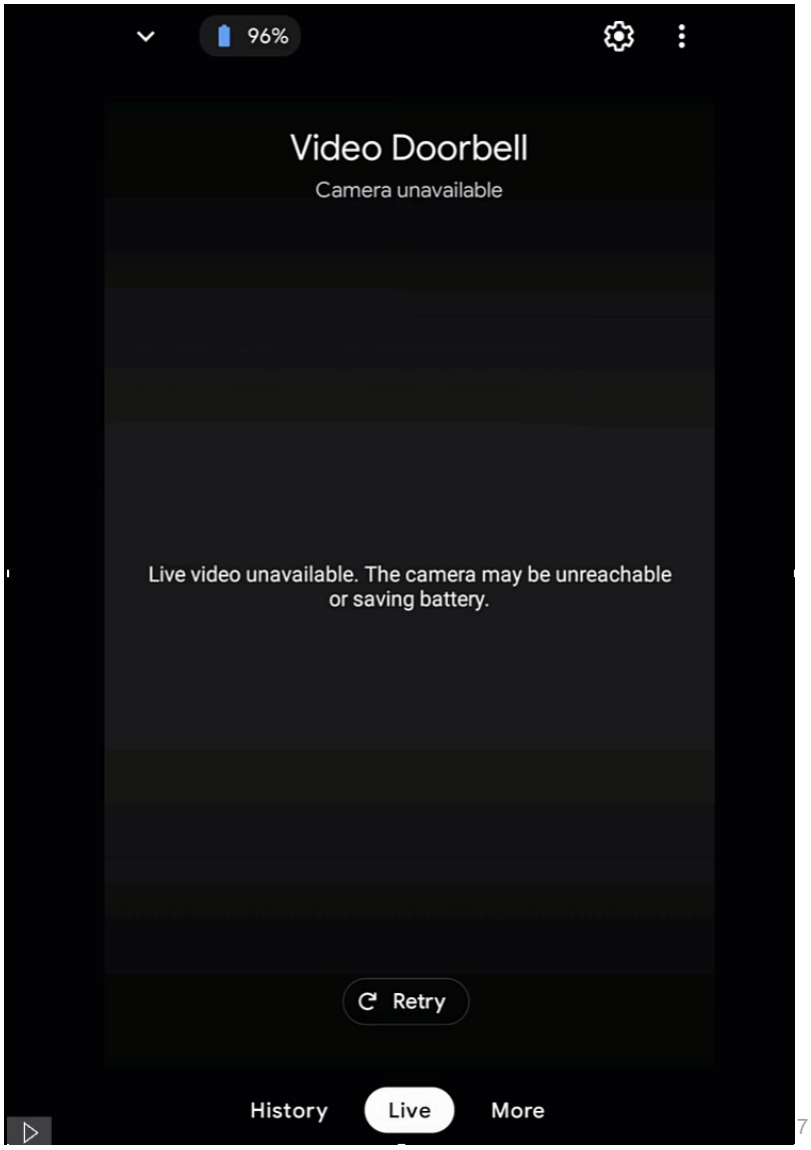
Attack crashes the entire communication chipset, disabling both BLE and WiFi – killing the video stream

KEYSIGHT

IOT Security Assessment in Action

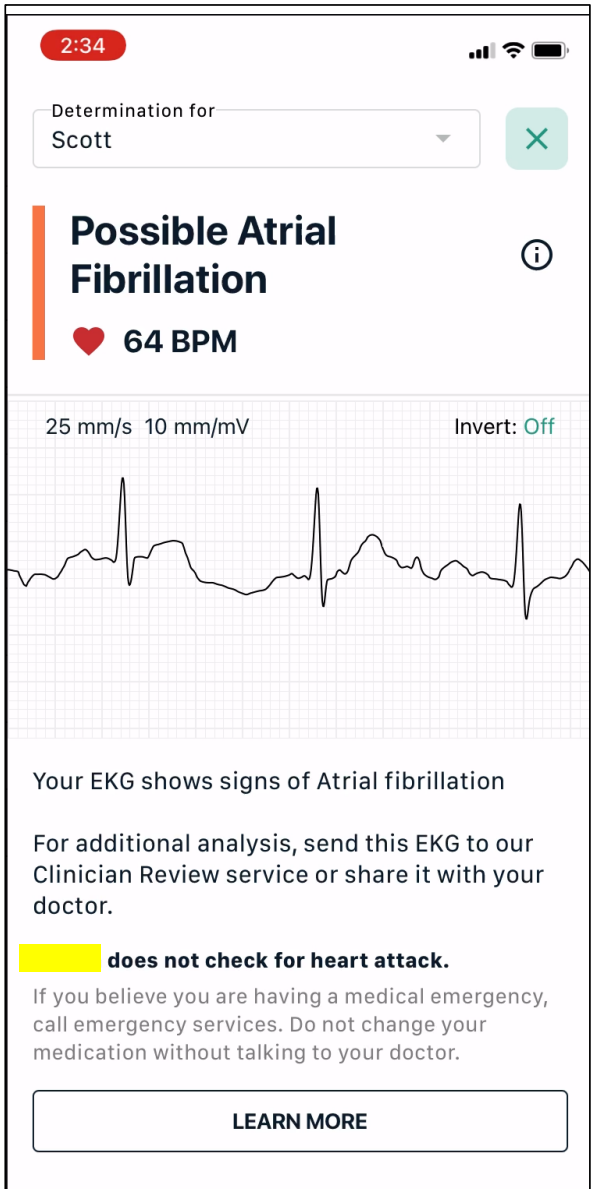
1. Target is a popular video doorbell streaming video over WiFi
2. Protocol Fuzzing attack targets the built-in Bluetooth Low Energy stack on the doorbell
3. Vulnerability is found, disrupting communication
4. Attack crashes the entire communication chipset, disabling both BLE and WiFi – killing the video stream

Time	State	Received Pkt	Reason	Fuzzed Pkt	Fuzzed Fields Name	Fuzzed Fields Value
2022-06-21 19_41_48.258578	FEATURE_RSP	BTLE / BTLE_DATA / CtrlPDU / LL_VERSION_IND	ANOMALY detected in state FEATURE_RSP	BTLE / BTLE_ADV / BTLE_SCAN_REQ	['RFU', 'unused', 'ScanA']	[[27036, 57431, '44:62:67:41:92:ef']]

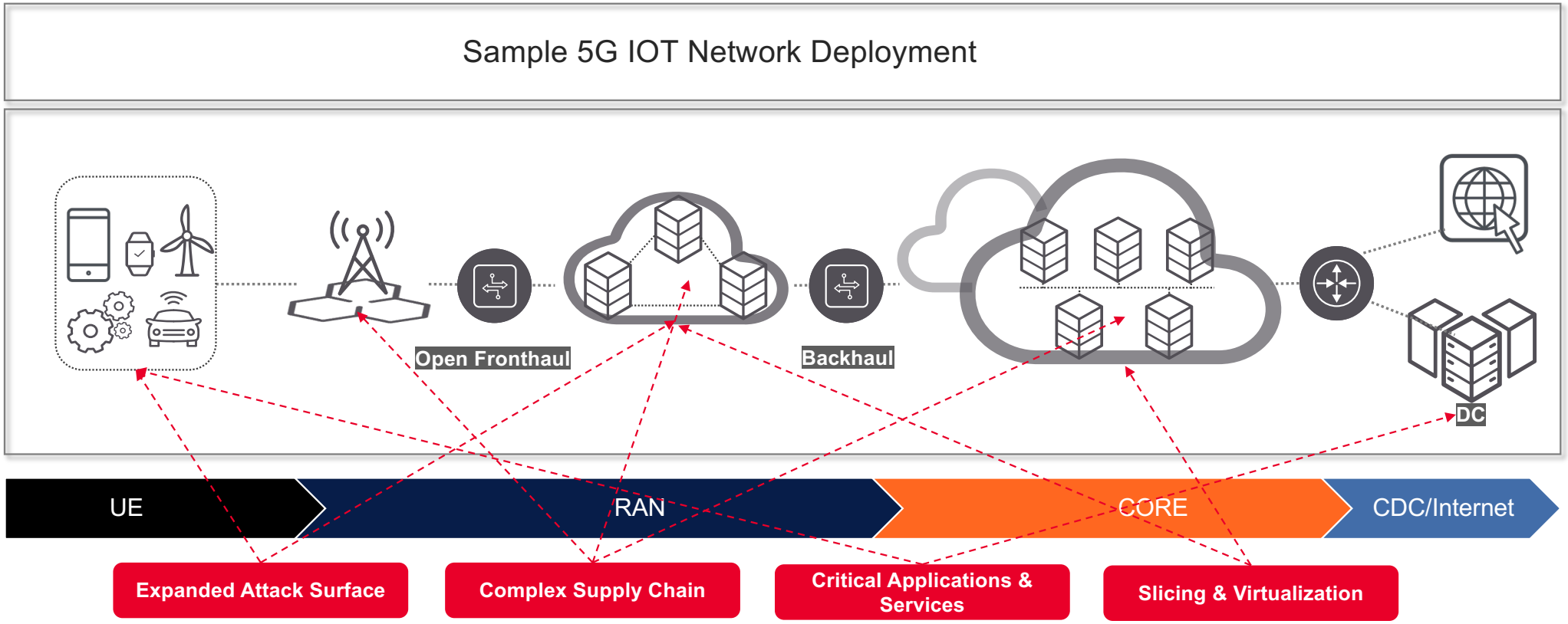


ECG Vulnerability

Attacking a heart monitor with a Bluetooth Low Energy attack by anyone within radio range causes it to display an incorrect medical diagnosis



The Brave New World



So What's the Solution?

Understand Security in YOUR Environment

Secure Design

Bake security in from day one, knowing devices will be globally connected

Compliance

Compliance isn't security, but it establishes a solid baseline and common standards

SBOM

Inventory of software libraries used to help w/ 3rd-party risk

Test

Pre- and post-deployment to understand risks in YOUR environment

KEYSIGHT

Thank you