Tracking Mass Vulnerabilities in IOT

By Cheryl Biswas

WHOAMI

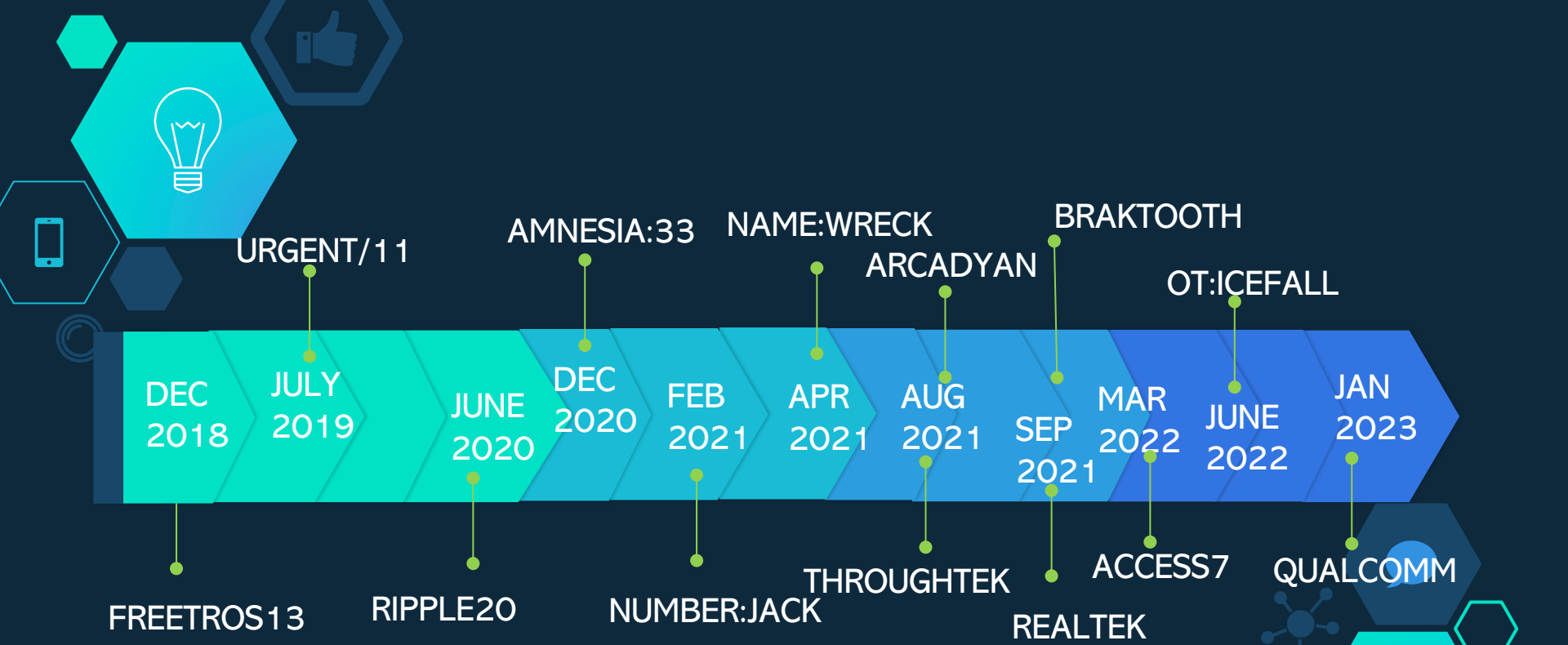
- Threat Intel Specialist with TD Bank
- Founding member of The Diana Initiative
- C3X College Student Cyber simulation
- Political Science Degree
- Cat mom
- “What if …”

Obligatory Disclaimer

The views expressed here are mine alone and not those of my employer

Agenda

- Defining Internet of Things
- IoT Architecture
- How Many Are There
- Attacks: It Only Takes One
- Make it Better, Please



"A Series of Unfortunate Events"

By Cheryl Biswas

Defining IoT

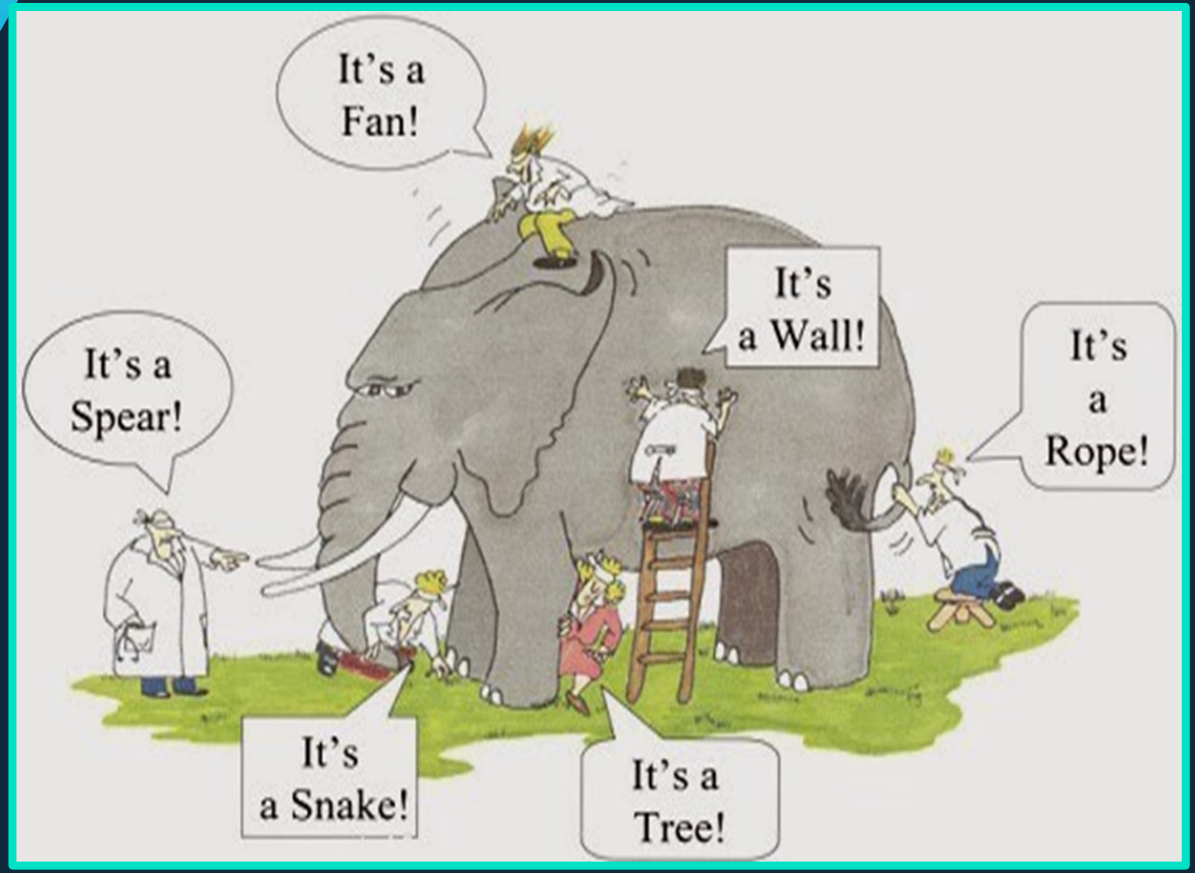
By Cheryl Biswas

A compromised IoT device on a corporate network can easily be used by attackers as a starting point for lateral movement and as a launchpad for attacks against other internal systems like servers and workstations that process sensitive data.

https://www.csoonline.com/article/3342207/iot-botnets-target-enterprise-video-conferencing-systems.html

By Cheryl Biswas

What we THINK IoT is



By Cheryl Biswas

Defining IoT

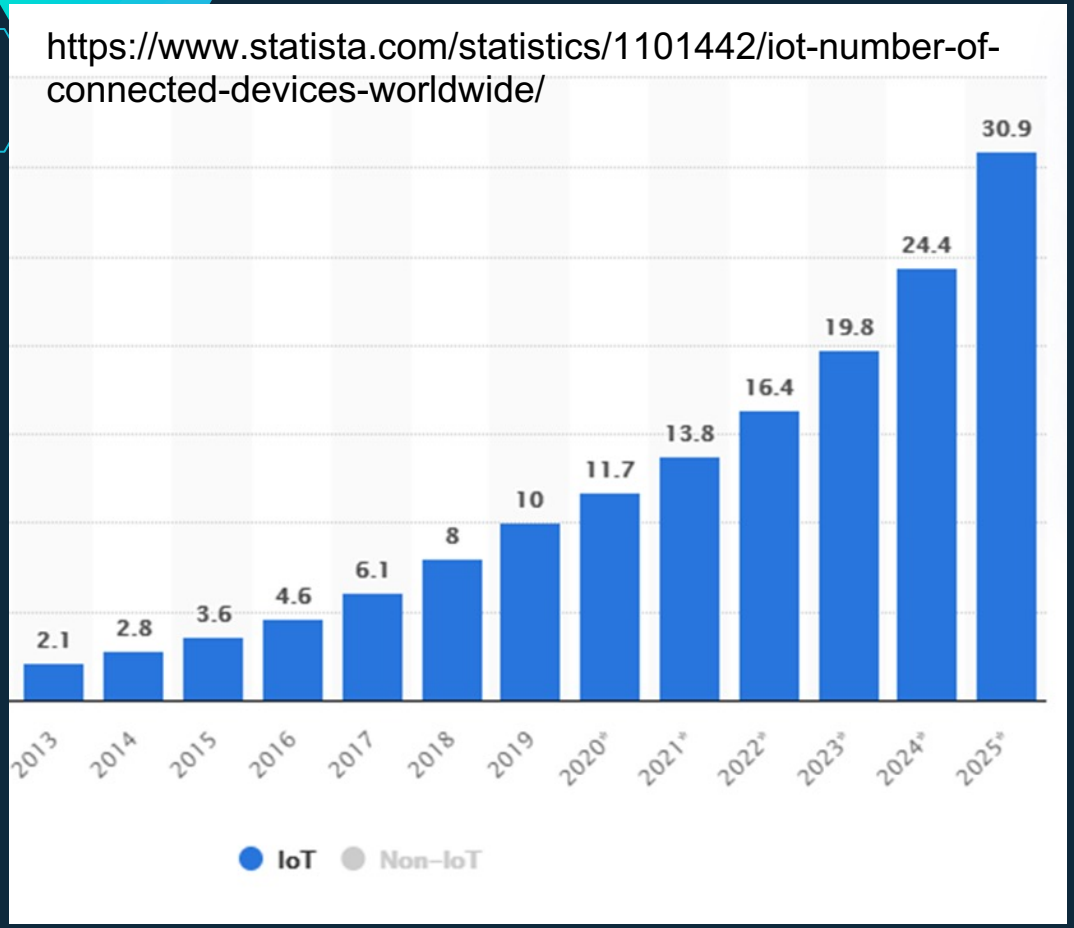
- Extend internet connectivity to physical devices
- Non-internet items connect online and communicate
- Multiple flavors: EIoT, IIoT, IoHT, IoT
- Machine to Machine or Mobile to Mobile
- Adding digital intelligence to “dumb” devices
- Enable communication without human intervention

What could go wrong?

By Cheryl Biswas

An Expanding Attack Surface

https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/



- 13.8 billion IoT endpoints in 2021
- 30.9 billion IoT devices in use by 2025
- *Exponential growth*

By Cheryl Biswas

IoT at Work

MEDICAL DEVICES	PATIENT MONITORING SYSTEMS, MOBILE IMAGING, INFUSION PUMPS, PACEMAKERS
OFFICE DEVICES & PERIPHERALS	PRINTERS, VOIP PHONES, BLUETOOTH KEYBOARDS, HEADSETS, SMART TVS AND MONITORS
BUILDING AUTOMATION	HVAC, SECURITY SYSTEMS, LIGHTING SYSTEMS, CAMERAS, VENDING MACHINES
CONSUMER DEVICES/WEARABLES	SMARTWATCHES, FITBITS, GAMING CONSOLES, APPLE TV, AMAZON EXHO, GOOGLE HOME, CARS
INDUSTRIAL & AGRICULTURAL DEVICES	PLCS, ROBOTIC ARMS, BARCODE SCANNERS, POS MACHINES, LOSS PREVENTION, SENSORS
IT INFRASTRUCTURE	ACCESS POINTS, ROUTERS, SWITCHES, FIREWALLS, BASEBOARD MGMT CONTROLLERS

IoT Architecture

By Cheryl Biswas

Talk amongst yourselves

- Device-to-device
- Device-to-cloud
- Device-to-gateway
- Cloud-to-cloud
- Wireless sensors and actuators connect the digital and physical realms

Communications

- LPWANS: low-power wide area network. Long range, cheap batteries, supported
- Cellular: $$$, power hungry
- Mesh Protocols: Zigbee. Short range, wireless, low power
- Bluetooth/low energy: BLE. Short range, low power for consumer IoT
- Wi-Fi: Poor scalability, power, coverage
- RFID: short distances for logistics, retail

IoT Architecture – 3 Layers

PERCEPTION LAYER: DEVICES

- Sensors, actuators, smart “things”
- Communicate to the cloud via wire or radio frequency RF

NETWORK LAYER: GATEWAYS

- The middleman
- Normalize, connect, transfer data between devices and cloud.

APPLICATION LAYER: THE CLOUD

- Data processing and storage
- Specialized services and functions

By Cheryl Biswas

Takeaways

- Three layers of architecture: Physical; Internet Gateway; Cloud
- Physical devices: billions of sensors and actuators that can produce a physical change
- Challenge: Monitoring data flow across three networks, third party APIs
- Integration issues: bringing evolving IoT tech into established enterprise environment

Hope is not a security strategy

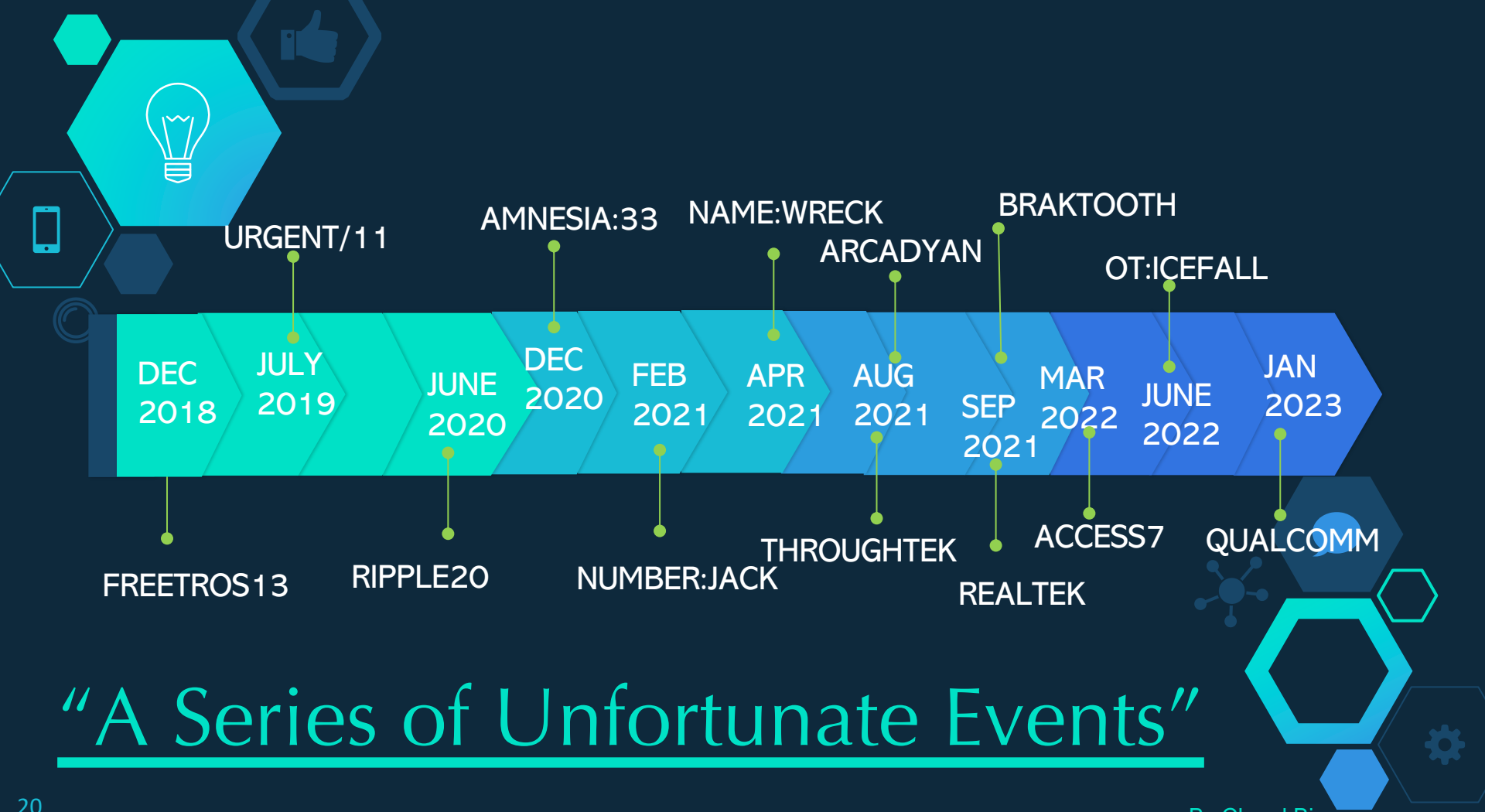
“Just because it hasn’t happened to you doesn’t mean it won’t”

Chris Romeo, Co-Founder and CEO Security Journey

By Cheryl Biswas

How Many are There

By Cheryl Biswas



"A Series of Unfortunate Events"

By Cheryl Biswas

Urgent /11 (07/2019)

- VxWorks TCP/IP stack IPnet
- 11 vulnerabilities, 6 critical enable RCE
- Affected versions span 13 years.
- **Impact:** Used in over 2 billion devices
- **Attacks:** Circumvent NAT and firewalls to control devices remotely via TCP/IP stack
- 97% of devices were unpatched December 2020
- UNDETECTED
- NO USER INTERACTION REQUIRED

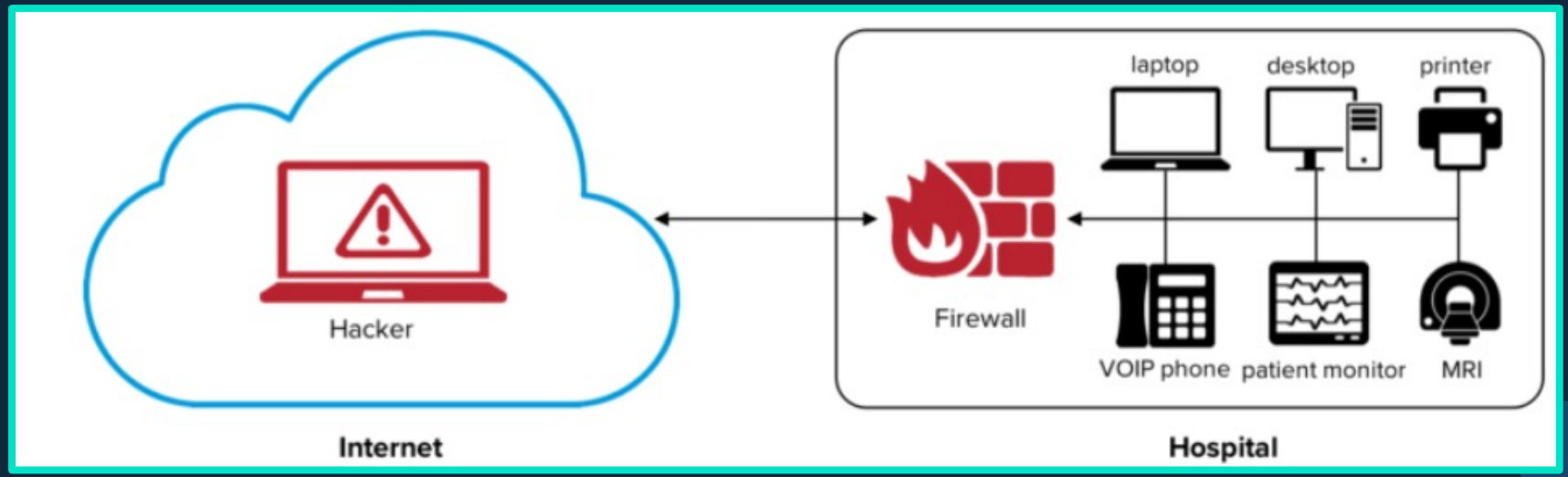
Urgent /11

- All VxWorks versions since 6.5
- SCADA devices
- Medical equipment: monitors, MRI machines
- Firewalls
- VOIP phones
- Printers
- Industrial controllers

By Cheryl Biswas

Urgent /11

Attacking Network Defences



ARMIS LINK
https://www.armis.com/research/urgent11

By Cheryl Biswas

Ripple20 (06/2020)

- Impacts the Treck TCP/IP library
- 19 vulnerabilities, 6 critical can enable RCE
- **Impact:** hundreds of millions of devices
- Healthcare, transportation, power grids
- Vendors: HP, Schneider Electric, Intel, Rockwell, Caterpillar, Baxter and more
- Complex or untracked supply chains
- Integrated into other software suites

How do you know if you use it?

Ripple20 (06/2020)

ATTACKS:

- Steal information from a printer
- Interfere with an infusion pump
- Impair industrial control device functions

"An attacker could hide malicious code within embedded devices for years. One of the vulnerabilities could enable entry from outside into the network boundaries"

www.jsof-tech.com/disclosures/ripple20

AMNESIA:33 (12/2020)

- 4 open source TCP/IP libraries:
  - uIP
  - FNET
  - picoTCP
  - Nut/Net
- 33 vulnerabilities impacting firmware
- 4 critical memory corruption flaws
- **Impact:** 150+ vendors, millions of consumer and industrial-grade devices

By Cheryl Biswas

AMNESIA:33

ATTACKS:

- Remote code execution
- Denial of Service
- Information leak
- DNS cache poisoning

IMPACTS:

- Sensors
- HVAC
- Printers
- IP cameras
- Self-checkout kiosks
- UPS
- RFID asset trackers
- Badge readers
- Routers
- Switches
- Game Consoles

By Cheryl Biswas

NUMBER:JACK (02/2021)

- Nine vulnerabilities in open source TCP/IP stacks
  - Adds 7 more stacks those from AMNESIA:33
- Improper generation of initial sequence numbers (ISNs)
- Attacks: DoS, authentication bypass or malicious code injection

"The prevalence of these stacks across embedded devices is significant"

Tenable

By Cheryl Biswas

CVE	Affected TCP/IP Stack	CVSSv3
CVE-2020-27213	**Ethernut (Nut/Net)**	7.5
CVE-2020-27630	uC/TCP-IP	7.5
CVE-2020-27631	CycloneTCP	7.5
CVE-2020-27632	NDKTCPIP	7.5
CVE-2020-27633	**FNET**	7.5
CVE-2020-27634	**uIP/Contiki-OS/Contiki-NG**	7.5
CVE-2020-27635	**picoTCP**	7.5
CVE-2020-27636	MPLAB Net	7.5
CVE-2020-28388	Nucleus NET	6.5

Flaw stems from weakness in TCP/IP Initial Sequence Number (ISN) generation

https://www.tenable.com/blog/numberjack-nine-vulnerabilities-across-multiple-open-source-tcpip-stacks#:~:text=Background,across%20embedded%20devices%20is%20significant.

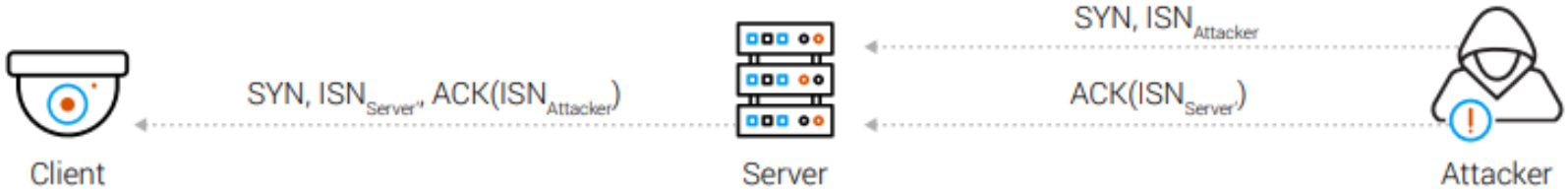


Figure 2 – ISN attack illustration

- Attacker impersonates Client. Opens connection to Server
- Server thinks SYN packet is from Client. Sends Client SYN-ACK
- Attacker guesses value of ISN Server. Sends ACK to Server
- Three-way handshake complete

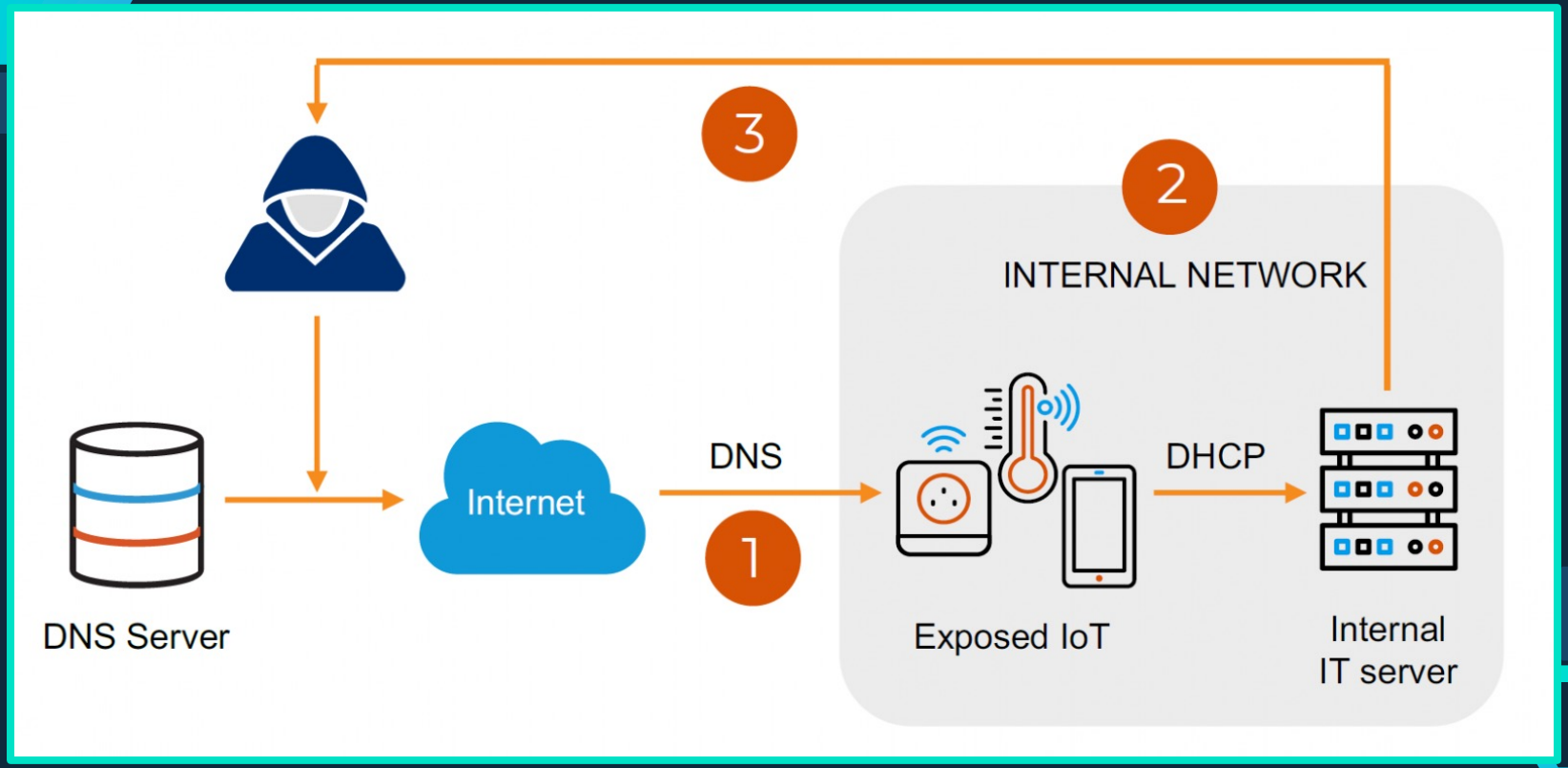
https://www.forescout.com/resources/numberjack-weak-isn-generation-in-embedded-tcpip-stacks/

NAME:WRECK (04/2021)

- Vulnerabilities related to DNS implementations
- Affects 4 popular TCP/IP stacks:
  - FreeBSD
  - IPNet
  - NetX
  - Nucleus NET
- **Impact:** 100 million enterprise and consumer devices, servers, network equipment, OT

By Cheryl Biswas

Attacks: DoS or RCE to control



https://www.bleepingcomputer.com/news/security/name-wreck-dns-vulnerabilities-affect-over-100-million-devices/

By Cheryl Biswas

REALTEK (04/2021)

- REALTEK SDK security flaws in RTL819xD chipsets
- 4 vulnerabilities:
  - CVE-2021-35392 stack buffer overflow via UPnP
  - CVE-2021-35393 heap-based buffer overflow
  - CVE-2021-35394 command injection
  - CVE-2021-35395 web interface flaws, remote arbitrary command execution
- Impact: 65 IoT device manufacturers, 200 product lines
- Affects WiFi devices: 100,000+ routers, cameras etc

By Cheryl Biswas

REALTEK (04/2021)

- **Attack:** Remote unauthenticated attack
- Execute arbitrary code at highest level of privilege
- Full compromise of a wireless router

"Given that wireless routers are a central 'node' for many devices, compromise here would spell disaster for other devices you have in your home and workplace"

Dray Agha, Security consultant, Jumpsec

Arcadyan (08/2021)

- CVE-2021-20090 Critical Authentication Bypass, trivial to exploit
- Arcadyan firmware in various home routers notably Buffalo
- **Impact:** Millions of devices, 20 vendors including ISPs
- List of affected routers and firmware versions here: https://www.lionic.com/news/2021/08/15/37-routers-have-the-highly-risky-cve-202120090-vulnerability/

Decade-old flaw, inherited down

Arcadyan Attacks

- Attacker can bypass authentication
- Access other devices on corporate networks
- Manipulate DNS records to deliver malicious content
- Attacks from China from February 2021, June-August 2021
  - Targeted vulnerable routers
  - Deployed Mirai botnet variant

Tenable Arcadyan PoC:

Modify device config to enable Telnet on vulnerable router and gain root shell access

Proof of Concept:

1. To get a valid httoken, navigate to http://<ip of device>/loginerror.html in a modern browser (tested on chrome).
2. Open DevTools
3. Run getToken() in the Console.
4. Copy the token, and use it in the following command from a terminal:

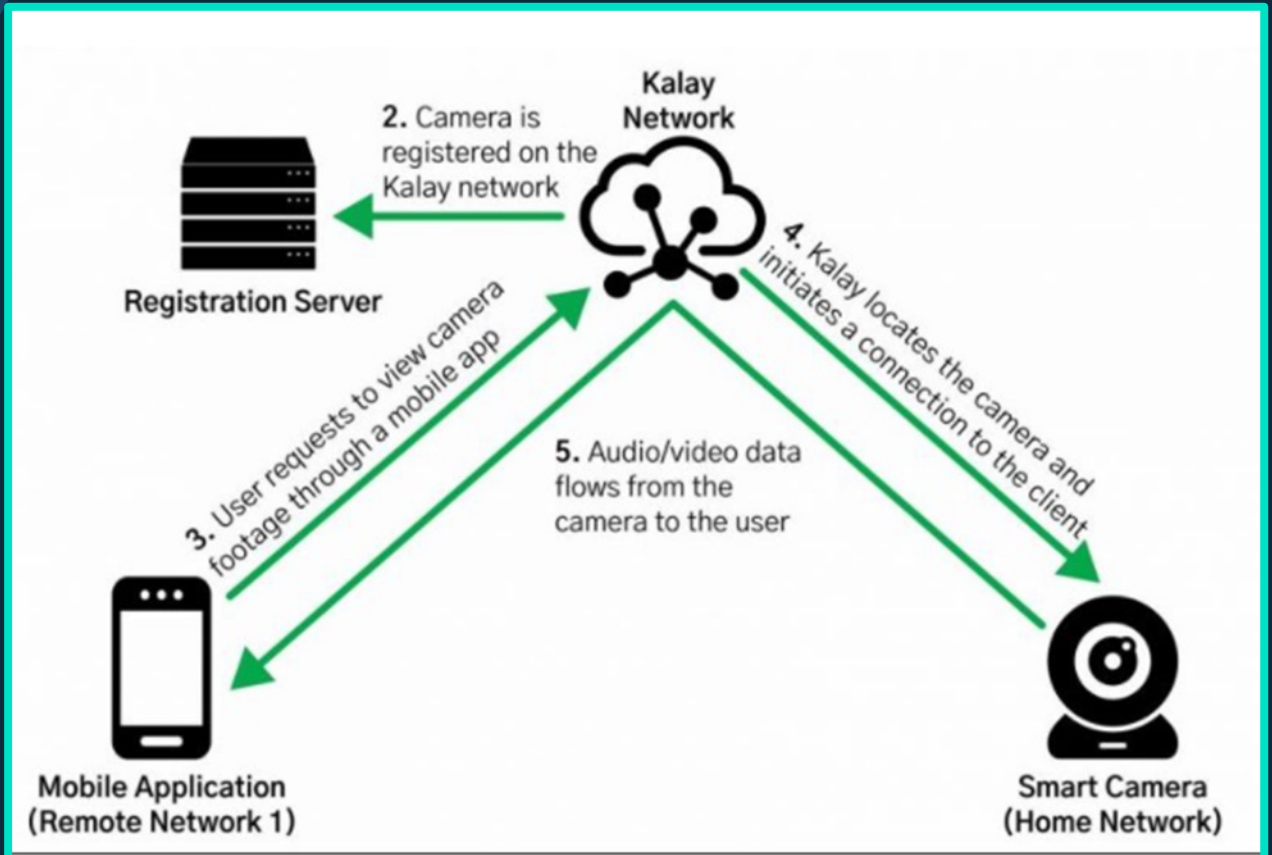
```
$ curl --include "http://192.168.11.1/cgi/cgi_i_filter.js?_tn=442853667" -H "Referer: http://192.168.11.1/loginerr

HTTP/1.1 200 OK
Date: Mon, 13 Jan 2020 15:24:03 GMT
Server: Arcadyan httpd 1.0
Content-type: application/x-javascript
X-FRAME-OPTIONS: SAMEORIGIN
Connection: close

/*DEMO*/
var login_password = "<admin password>";

addCfg("lan_ipaddr", 0, "192.168.11.1");
```

https://www.tenable.com/security/research/tra-2021-13

By Cheryl Biswas

ThroughTek (08/2021)

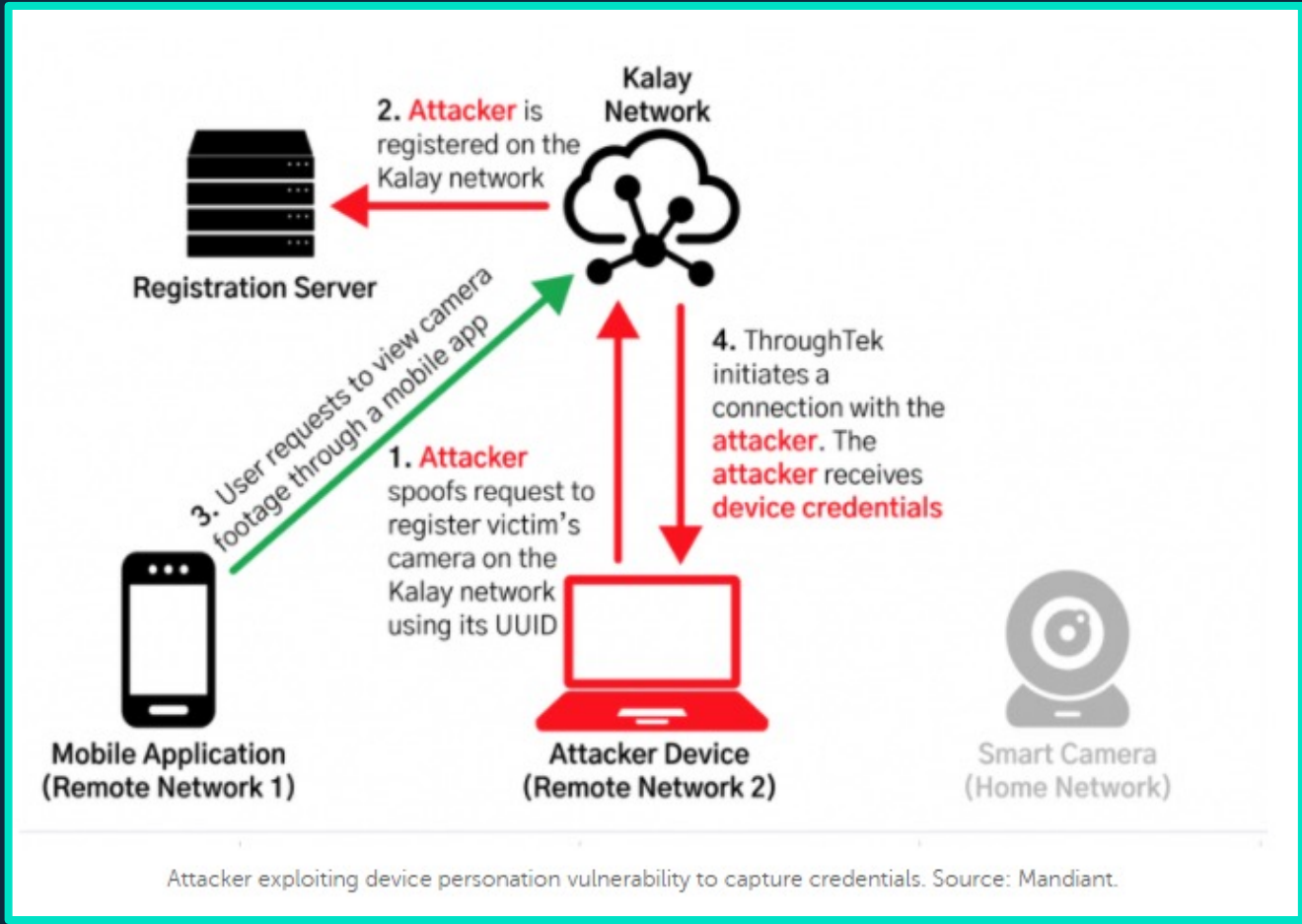
- CVE-2021-28372 Improper access control flaw in ThroughTek point-to-point (P2P) products
- Kalay P2P Software Development Kit (SDK)
- 83 million devices on Kalay platform
- Supply chain impact to OEMs of security cameras and IoT
- Attack: remote attacker could control vulnerable device for RCE
- CISA advisory for RCE and unauthorized access to sensitive information



Kalay flow. Source: Mandiant.

https://threatpost.com/bug-iot-millions-devices-attackers-eavesdrop/168729/

By Cheryl Biswas



Attacker exploiting device personation vulnerability to capture credentials. Source: Mandiant.

https://threatpost.com/bug-iot-millions-devices-attackers-eavesdrop/168729/

By Cheryl Biswas

BrakTooth (09/2021)

- 16 vulnerabilities across 13 Bluetooth chipsets
- Most severe: CVE-2021-28139.
- Affects ESP32 SoC used in many Bluetooth based appliances
- 1400 products 11 vendors: Intel, Qualcomm, TI, etc
- Attacks: crash or deadlock
- No previous pairing or authentication required

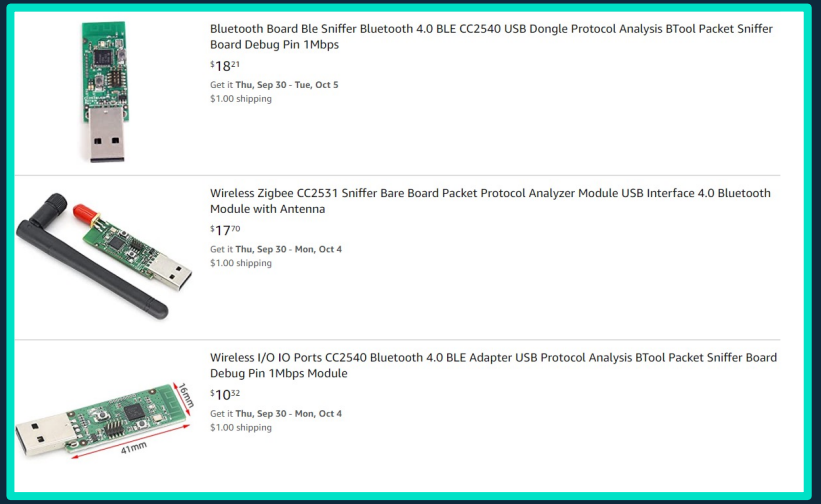
BlueTooth

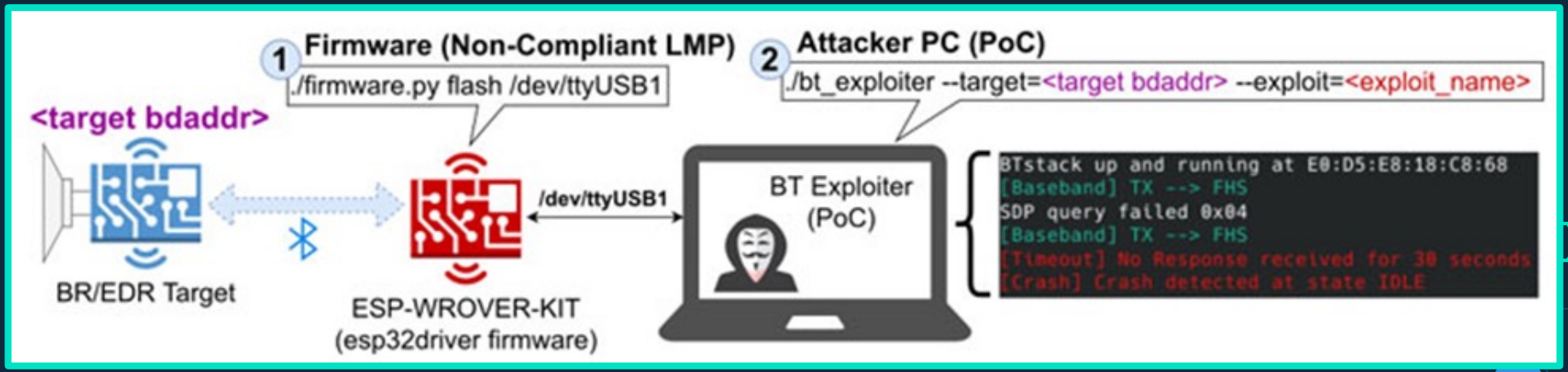
Other Bluetooth protocol vulnerabilities from 2019:

- BLESA
- BLURtooth
- BIAS
- SweynTooth
- KNOB

ATTACKS:

- Code injection
- Erase NVRAM data
- $15 Bluetooth USB radio kit





By Cheryl Biswas

BrakTooth Patching

Table 5: Patching status, Vulnerabilities and SDK/Firmware version of affected devices.

* Contact vendor to acquire the patch.

SoC or Module Vendor	BT SoC	Firmware or SDK Ver.	Vuln. / Anomalies	Patch Status
Espressif Systems	ESP32	esp-idf-4.4	V1,V3-4 / A1	[35, 12] **Available**
Intel	AX200	Linux - ibt-12-16.ddc Windows - 22.40.0	V15-16 / A1-2, A5	Patch in progress
Qualcomm	WCN3990/8	crbtfw21.tlv, patch 0x0002	V15 / A1-2,A4	Patch in progress
Qualcomm	CSR8811/CSR8510	v9.1.12.14	V6 / A1-2	No fix
Texas Instruments	CC2564C	cc256xc_bt_sp_v1.4	V12 / A1-2	No fix
Infineon (Cypress)	CYW20735B1	WICED SDK 2.9.0	V12-15 / A2,A6	[17] **Available**
Bluetrum Technology	AB5301A	V06X_S6645 (LMP Subver. 3)	V7,V12 / A1-2	**Available** *
Zhuhai Jieli Technology	AC6925C	*unspecified* (LMP Subver. 12576)	V8-9 / A1-2	Investigation in progress
Zhuhai Jieli Technology	AC6905X	*unspecified* (LMP Subver. 12576)	V5,V8-9 / A1-2	Investigation in progress
Zhuhai Jieli Technology	AC6366C	fw-AC63_BT_SDK 0.9.0	V2,V12 / A1-2	Patch in progress
Actions Technology	ATS281X	*unspecified* (LMP Subver. 5200)	V4,V10-11 / A1-2	Investigation in progress
Harman International	JX25X	*unspecified* (LMP Subver. 5063)	V4 / A1-2	Pending
Silabs	WT32i	iWRAP 6.3.0 build 1149	V5 / A1-2	Pending

Table 5 captures the affected vendors and the status of their investigation. We categorize the status of the investigation in the following forms:

- ***Available***: The vendor has replicated the vulnerability and a patch is available.
- ***Patch in progress***: The vendor has successfully replicated the vulnerability and a patch for the same will be available soon.
- ***Investigation in progress***: The vendor is currently investigating the security issue and our team is assisting them.
- ***No fix***: The vendor has successfully replicated the issue, but there is no plan to release a patch.
- ***Pending***: The vendor hardly communicated with the team and the status of their investigation is unclear at best.

Code to test: https://asset-group.github.io/disclosures/braktooth/

Qualcomm SnapDragon (01/2023)

- Qualcomm SnapDragon processor chips
- 22 vulnerabilities, 2 are critical
  - CVE-2022-33265, 33219,
- Impact: cars, powerline communications
- UEFI ARM firmware CVE-2022-40516-40520
- All ARM-based laptops and devices
- https://docs.qualcomm.com/product/publicresources/securitybulletin/january-2023-bulletin.html

Qualcomm SnapDragon

- Attackers seek less hardened targets: firmware. Conti
- Vulnerabilities in reference code affect the whole ecosystem. Multiple vendors, multiple product lines
- Downstream impact: Lenovo computers
- Powerline communications: complicated & $$$ to fix

”First massive public disclosure related to UEFI firmware on ARM”

SC Magazine: Qualcomm, Lenovo flag multiple high impact firmware vulnerabilities

Takeaways

- Series of widespread vulnerabilities related to TCP/IP stacks
- TCP/IP stack flaws are inherited from software used in embedded devices
- The problem of identification
- Embedded devices are hard to manage & update
- Attackers search for unpatched vulnerabilities to exploit

Is this in my device? Is this on my network?

In other words, the smart device ecosystem remains a mess and will most likely remain a security disaster for years to come… all of this comes down to bad coding practices, such as an absence of basic input validation and shotgun parsing, the primary issues at the heart of the Urgent/11, Ripple20, and Amnesia:33 vulnerabilities

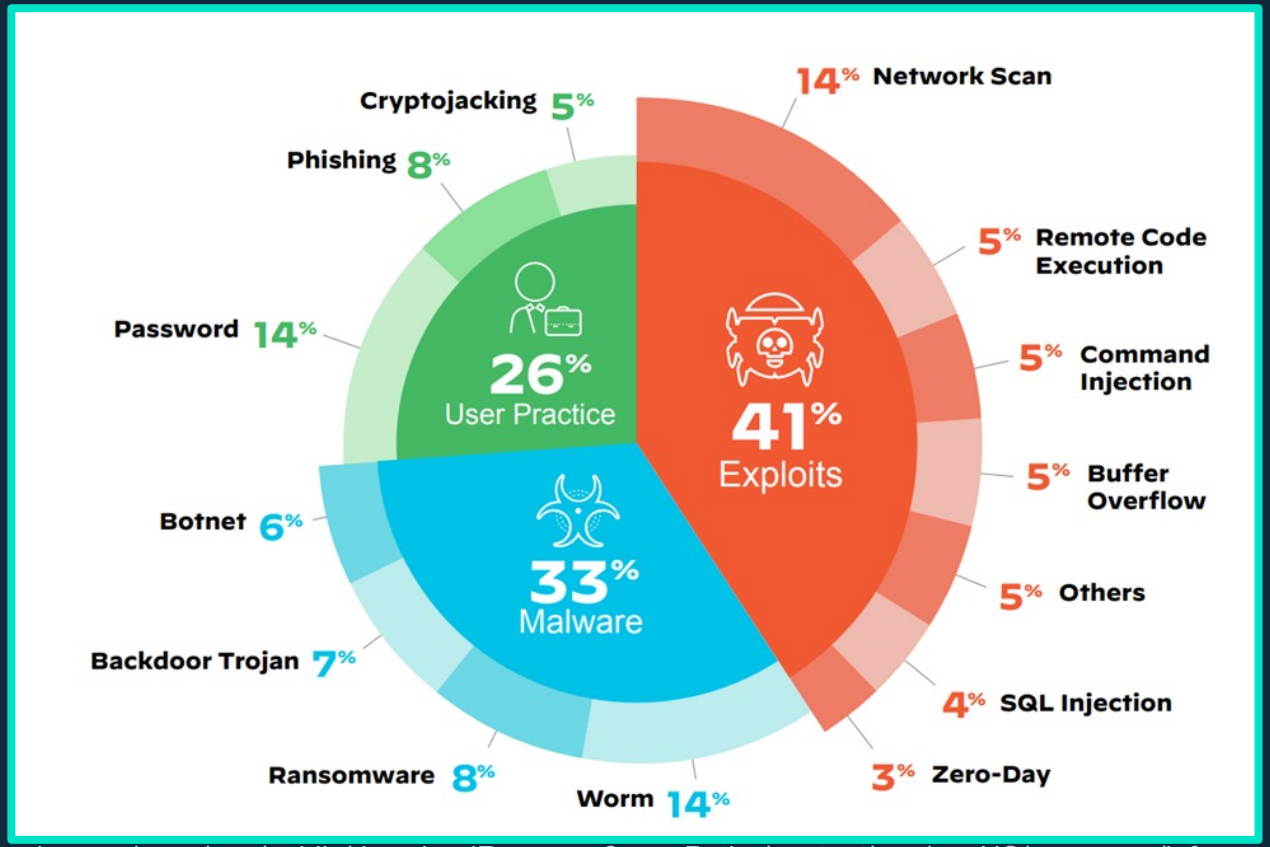
https://www.zdnet.com/article/amnesia33-vulnerabilities-impact-millions-of-smart-and-industrial-devices/

By Cheryl Biswas

Attacks: It Only Takes One

By Cheryl Biswas

Wheel of Mis-Fortune



https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/infographics/state-of-enterprise-iot-security-in-2020

By Cheryl Biswas

We Have Issues

- 98% of EIoT communications are in plain text
- 57% vulnerable to medium-high severity attacks
- 83% medical imaging devices run unsupported OS
- Most organizations now have IT/OT/IoT mix
- 24% connected devices in organizations not traditional IT
- 76% exploits target software libraries eg Log4j
- https://www.forescout.com/blog/2022-threat-roundup-the-emergence-of-mixed-itiot-threats/

We Have Issues

- IoT is not scalable
- Misconfiguration
- No centralized control over IoT devices & apps
- Shadow IoT: 1000s of devices connect to enterprise networks daily
- Security is **not** an add-on
- Lack of visibility. We're not looking for it

You don't know what you've got til it's pwned

Strontium Attack

- April 2019 Russian APT28 Strontium
- Targeted attack on IoT devices
- Multiple customer locations for initial access to corporate networks
- Attempted exploits against a VOIP phone, printer, and video decoder
- **Factory security settings on 2 devices**
- **Software not updated on another device**

Polycom

Have you ever been on a conference call where you really wished you could take command of the situation? With Metasploit Framework and the new Polycom HDX exploit, you can (if given permission by the owner of the device, that is)! If teleconferencing isn't your target's style, you can also pwn correspondence the old-fashioned way: through a Microsoft Office exploit. Be it written or video, we here at Rapid7 know you value other people's communication!

By Cheryl Biswas

Takeaways

- IT Security, attack scenarios, threat models don't apply
- Unmanaged IoT more vulnerable to attack
- Shadow IoT an ongoing and increasing risk
- Use automation to reduce misconfiguration
- Network segmentation required

What's on your network?

5

Make it Better, Please

By Cheryl Biswas

By Cheryl Biswas

Legislation / Regulation

- January 2020 California IoT Cybersecurity Improvement Act (2017)
- European Union Agency for Cybersecurity (ENISA) recommendations
- European Telecommunications Standards Institute (ETSI) standards
- December 2020 IoT Cybersecurity Improvement Act
- March 2021 NIST Cybersecurity Standards for IoT

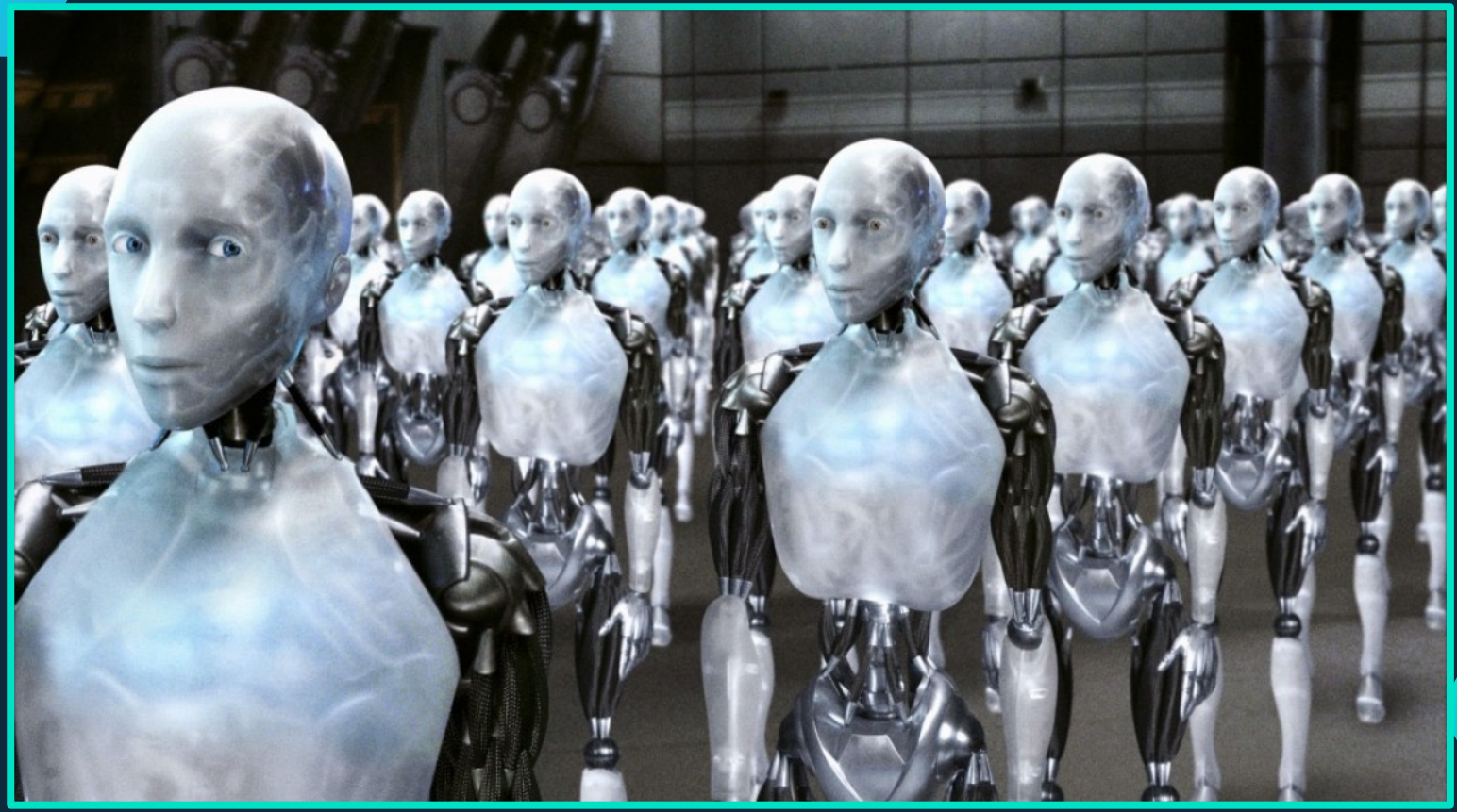
IoT Policy and Compliance

- Asset inventory of ALL the things
- Device classification and risk assessment
- Use frameworks from NIST and CIS
- Develop a comprehensive IoT security policy
- Data encryption all the time
- Have a mature SDLC
- *BOMs: Bills of Material for Software, Hardware, Firmware

Get the Basics Right

- Know your attack surface
- Strong authentication – multi-factor
- Network segmentation – it only works if we do it
- Firewalls and VPNs - patched
- Automation
- Centralize access logs
- Behavior monitoring
- Zero Trust

Or this will end badly



By Cheryl Biswas

Thank You!

Any questions?

You can find me at:

- Twitter: @3ncr1pted