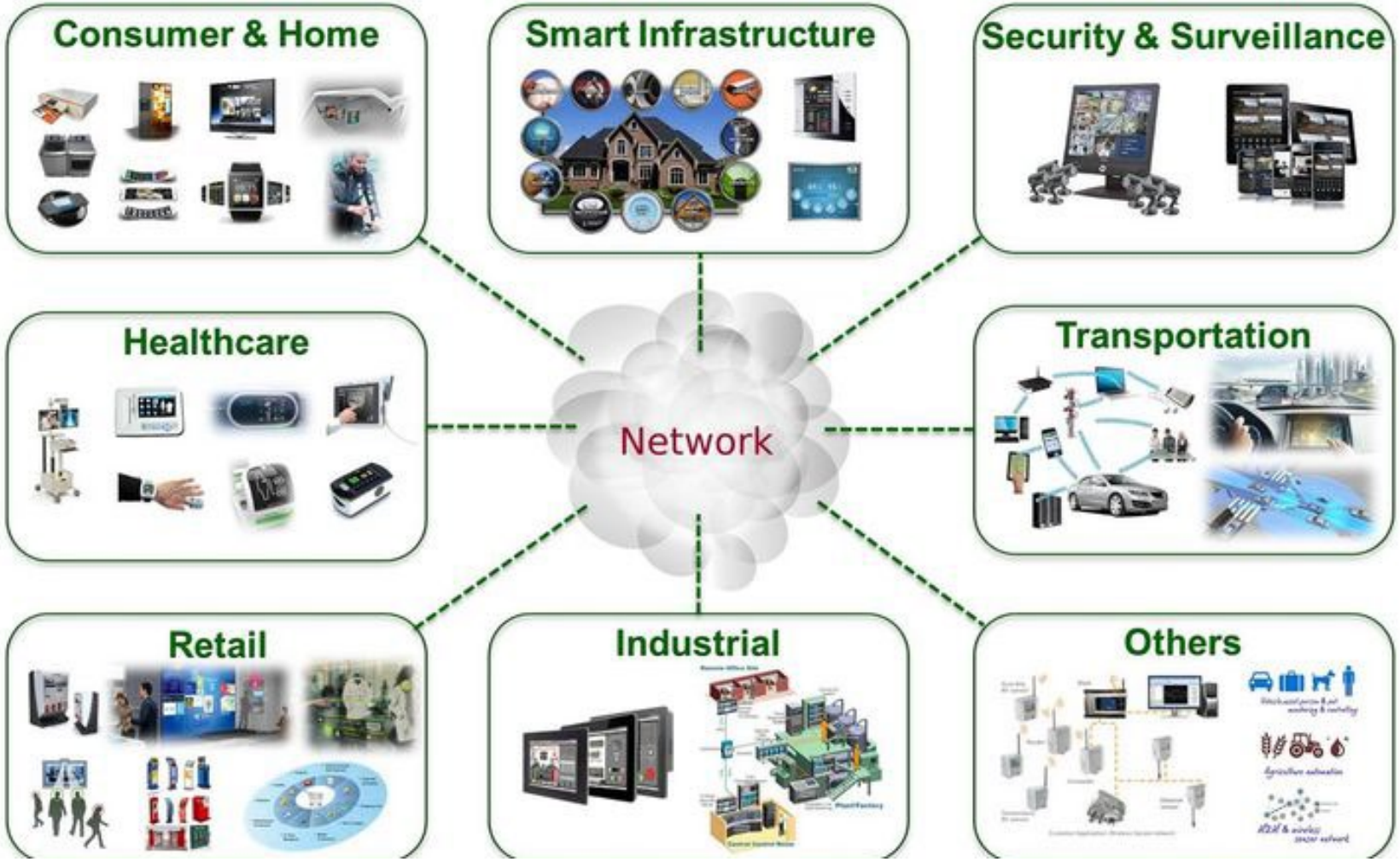
18.1 IOT OVERVIEW

- IOT
- Application Areas and Devices

WHAT IS THE INTERNET OF THINGS (IOT)?

- AKA Internet of Everything
- IoT can best be thought of as:
  - The process of connecting everyday objects and systems to a network (Internet)
  - Makes all devices globally available and interactive
- Includes devices from all sectors
- There are currently over 12 billion IoT devices connected to the Internet
  - In 2025 that number is expected to reach nearly 40 billion

IOT EXAMPLE


Consumer & Home
Smart Infrastructure
Security & Surveillance
Healthcare
Network
Transportation
Retail
Industrial
Others

IOT APPLICATION AREAS AND DEVICES

Service Sector	Application Group	Location	Devices
Buildings	• Commercial • Industrial	• Office • Education • Retail • Hospitality • Healthcare • Airports • Stadiums	• HVAC • Transport • Fire & Safety • Lighting • Security • Access
Energy	• Supply/Demand • Oil/Gas • Alternative	• Power generators • Transportation & Distribution • Low Voltage • Power Quality • Energy management • Solar & Windmills • Electrochemical • Rigs, derricks, pumps • Pipelines	• Turbines • Windmills • UPS • Batteries • Generators • Meters • Drills • Fuel Cells

IOT APPLICATION AREAS AND DEVICES (CONT'D)

Service Sector	Application Group	Location	Devices
Consumer and Home	• Infrastructure • Awareness & Safety • Convenience and Entertainment	• Wiring, network access, energy management • Security/Alerts, Fire safety, Elderly, Children, Power protection • HVAC/Climate, Lighting, Appliances, Entertainment	• Cameras, power systems, e-Readers, dishwashers, desktop computers, washers/dryers, meters, lights, TVs, MP3 players, Gaming consoles, alarms
Healthcare and Life Sciences	• Care • In Vivo/Home • Research	• Hospital, ER, Mobile, PoC, Clinic, Labs, Doctor's office • Implants, Home, monitoring systems • Drug discovery, diagnostics, labs	• MRI, PDAs, Implants, health monitors, Surgical Equipment, Pumps, Monitors, Telemedicine

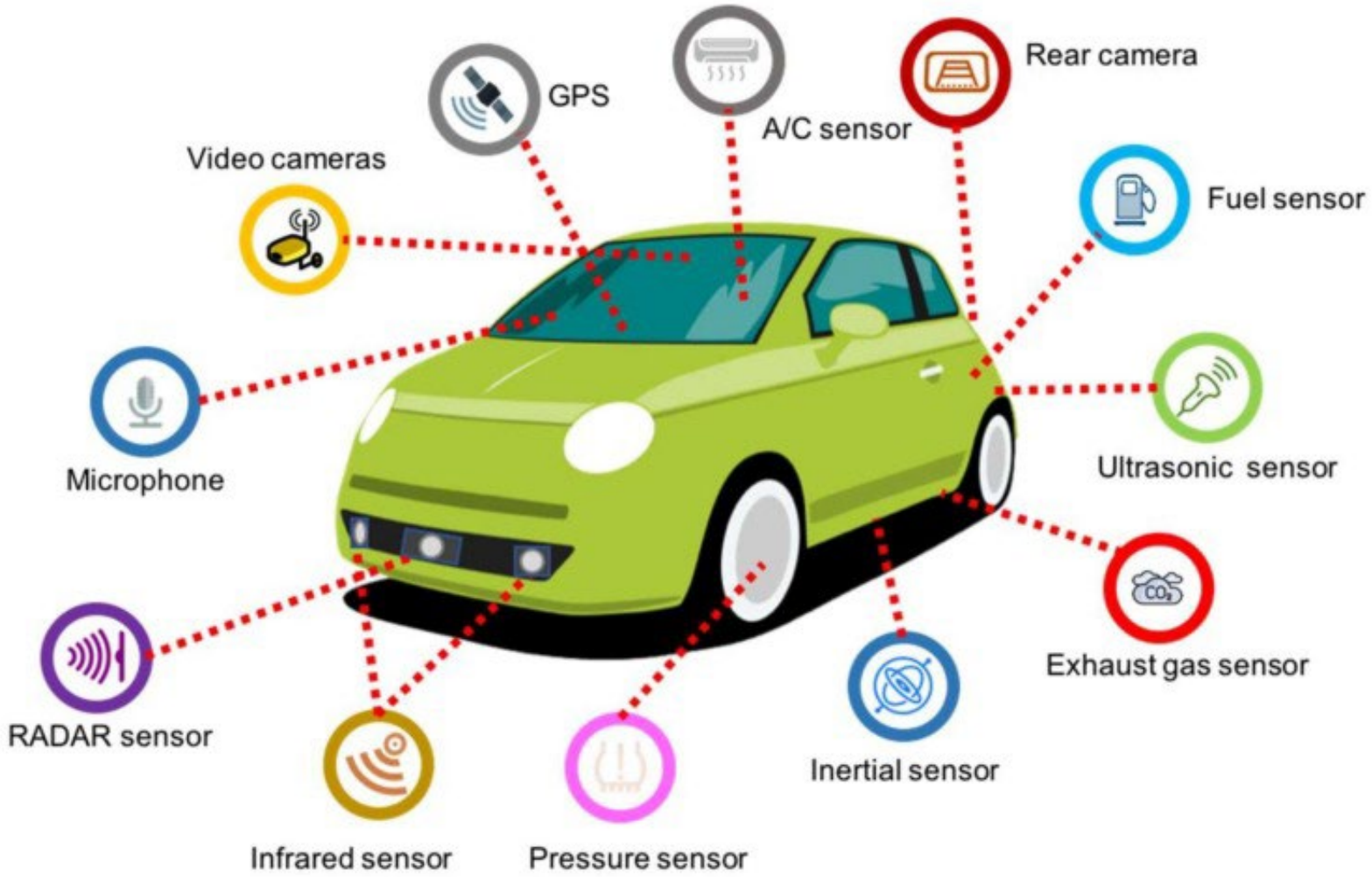
SMART HOME IOT EXAMPLE

IOT ENHANCED SURGICAL THEATER

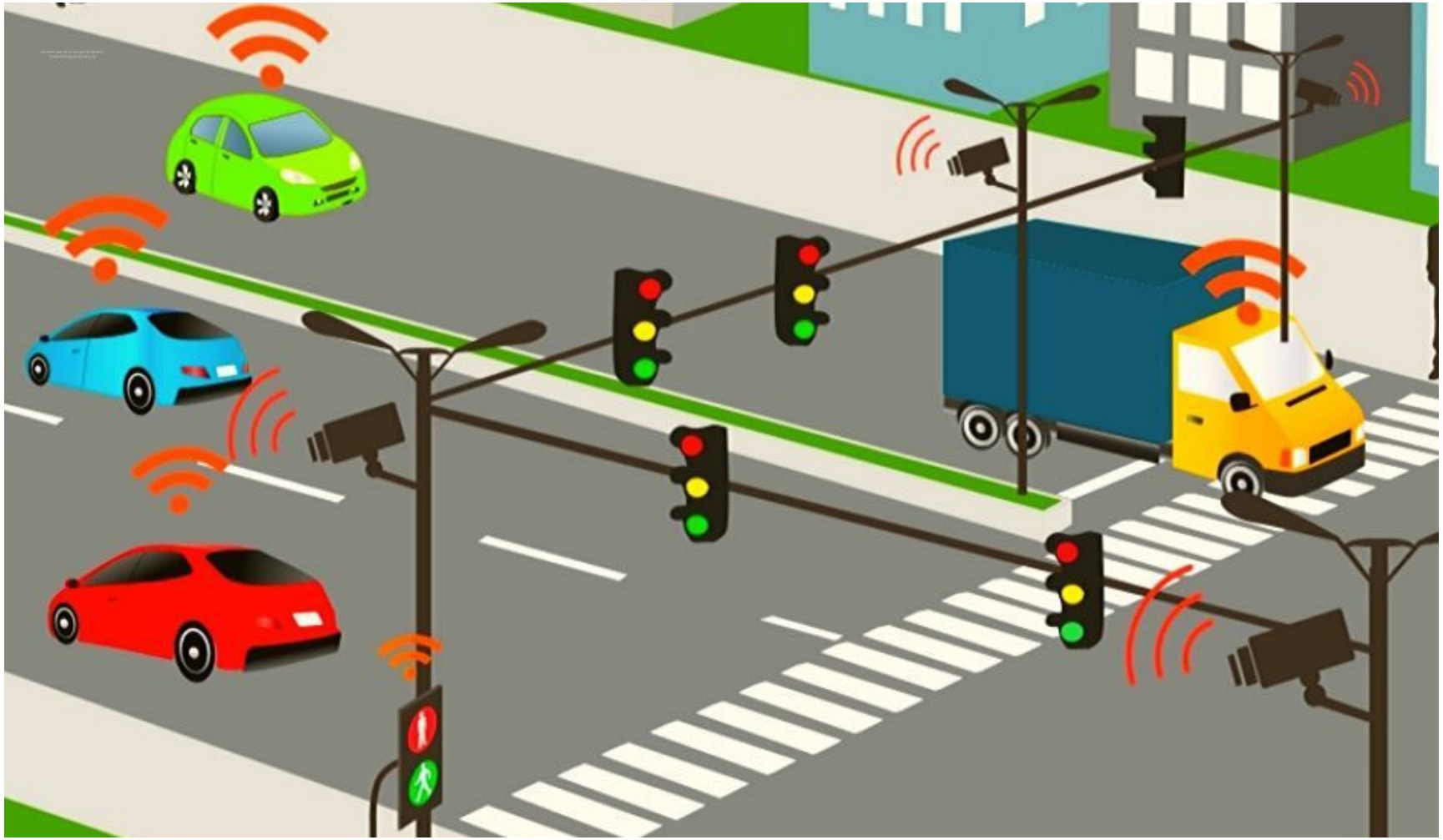
IOT APPLICATION AREAS AND DEVICES (CONT'D)

Service Sector	Application Group	Location	Devices
Transportation	• Non-Vehicular • Vehicles • Transportation Systems	• Air, Rail, Marine • Consumer, Commercial, Construction, Off-Highway • Tools, traffic management, navigation	• Vehicles, lights, ships, planes, signage, tolls
Industrial	• Resource automation • Fluid/Processes • Converting/Discrete • Distribution	• Mining, irrigation, agriculture, woodland • Petrochemical, hydro, carbons, food, beverage • Metals, papers, rubber/plastic • Metalworking • Electronics • Assembly/testing	• Pumps, valves, vats, conveyors, fabrication, assembly/packaging, vessels, tanks

AUTOMOTIVE IOT



IOT IN TRANSPORTATION EXAMPLE

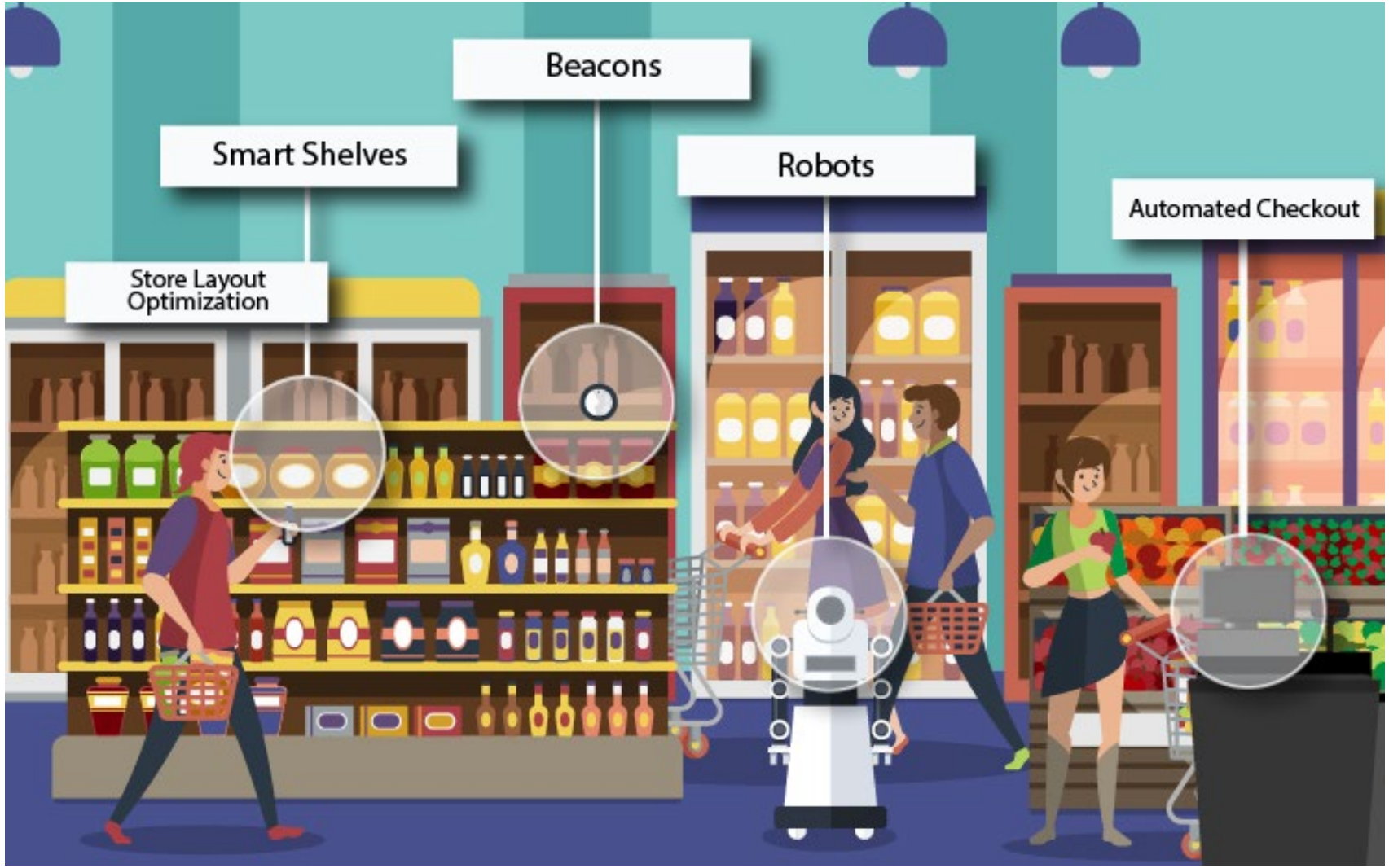


IOT APPLICATION AREAS AND DEVICES (CONT'D)

Service Sector	Application Group	Location	Devices
Retail	• Specialty • Hospitality • Stores	• Fuel stations, Gaming, Bowling, Cinemas, Discos, Special Events, • Hotel restaurants, bars, cafes, clubs • Supermarkets, shopping centers, single site, distribution	• POS Terminals, Tags, Cash Registers, Vending machines, Signs, inventory control
Security / Public Safety	• Surveillance • Equipment • Tracking • Public Infrastructure	• Radar/satellite, environmental, military, unmanned, fixed • Human, animal, postal, food, health, beverage • Water treatment, building, environmental equipment, personnel, police, fire, regulatory	• Tanks, fighter jets, battlefields, jeeps, cars, ambulance, Homeland security, Environment, Monitoring

IOT IN RETAIL EXAMPLE

SMART STORE EXAMPLE

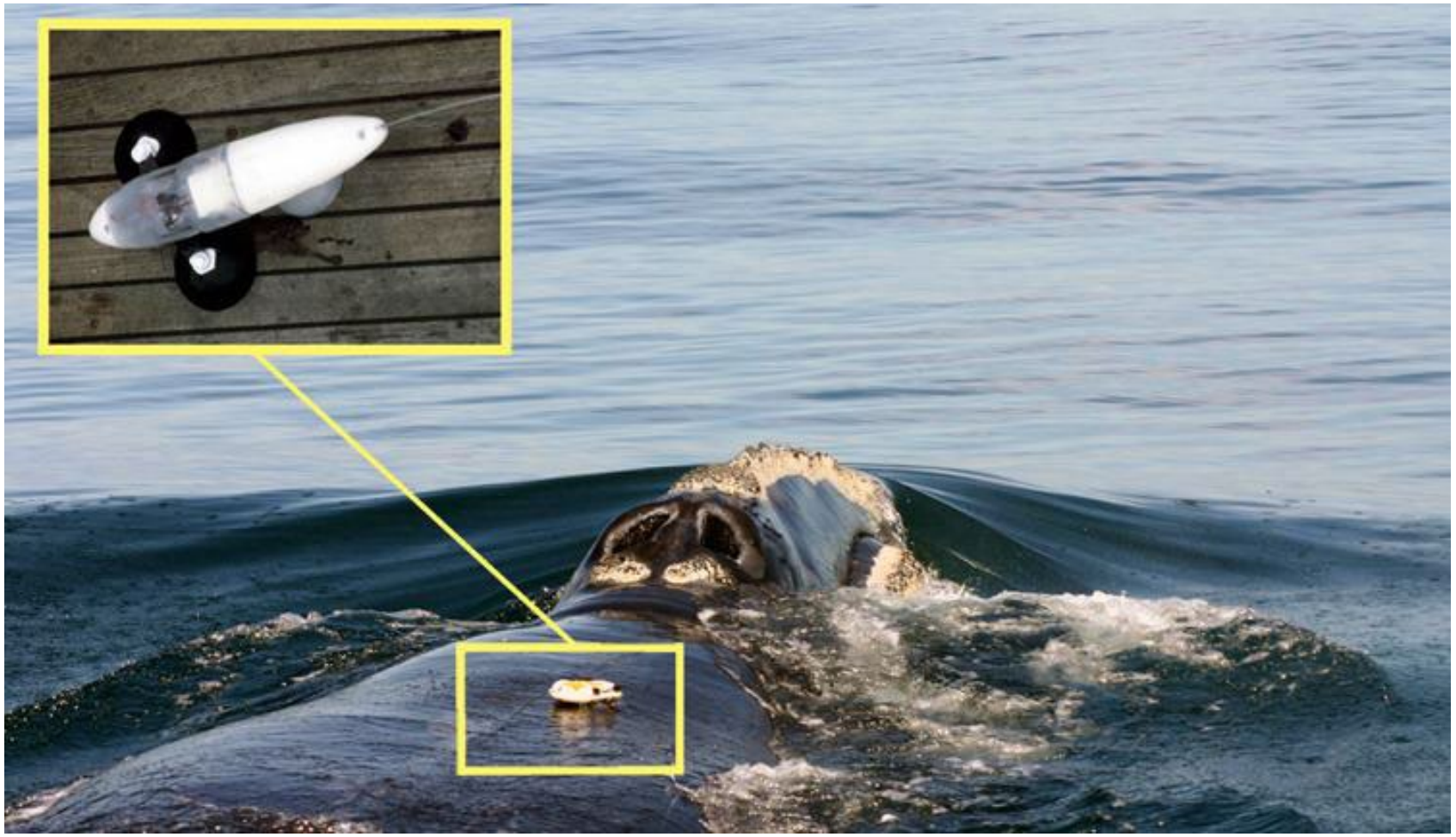


IOT APPLICATION AREAS AND DEVICES (CONT'D)

Service Sector	Application Group	Location	Devices
IT and Networks	• Public • Enterprise	• Services, e-Commerce, data centers, mobile carriers, ISPs	• Servers, storage, PCs, routers, switches, wireless access points, PBXs
Scientific	• Research • Public health and safety initiatives monitoring and analysis	• Closed laboratory • Outdoor (Earth) environment	• Oceanic, atmospheric, and land condition sensors • Animal trackers • Lab environment sensors and actuators

IOT CONSERVATION TRACKING EXAMPLE

IOT SCIENTIFIC RESEARCH EXAMPLE



IOT APPLICATION AREAS AND DEVICES (CONT'D)

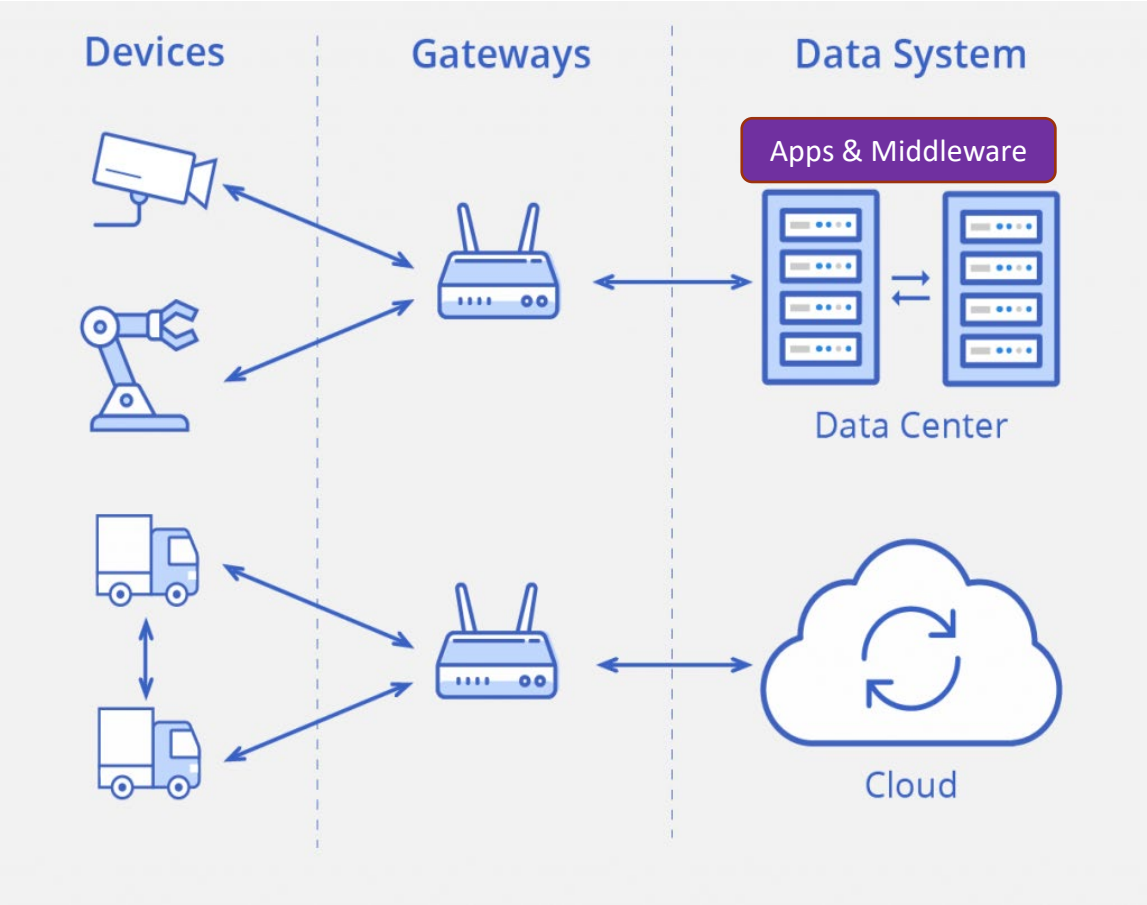
Service Sector	Application Group	Location	Devices
Agriculture	• Precision Farming • Livestock Monitoring • Reduction of resource wastage	• Farms • Greenhouses • Livestock areas	• Animal wearables • Drones • Soil, irrigation, environmental sensors and actuators

18.2 IOT INFRASTRUCTURE

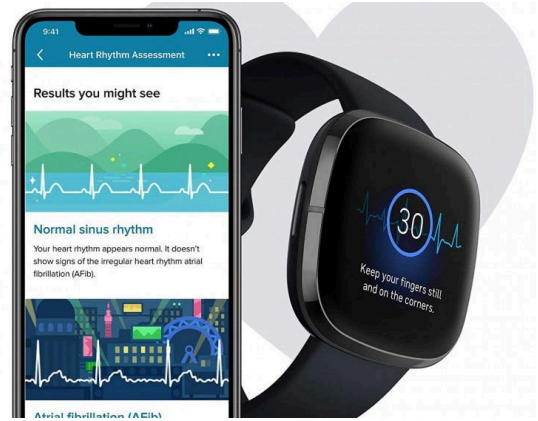
- Architecture
- Communication
- Network Scopes
- Network Protocols

IOT ARCHITECTURE

- End Devices
  - Sensors, RFID tags, readers
  - Gather telemetry
- IoT Gateway
  - Connects device to the cloud
- Cloud Server/Data Center
  - Connect through web services
  - Data processing and storage
  - Processed data transmitted back to the user
- Remote Control
  - End user uses a mobile app
  - Monitor, control, retrieve data, take an action
  - User can be in a remote location

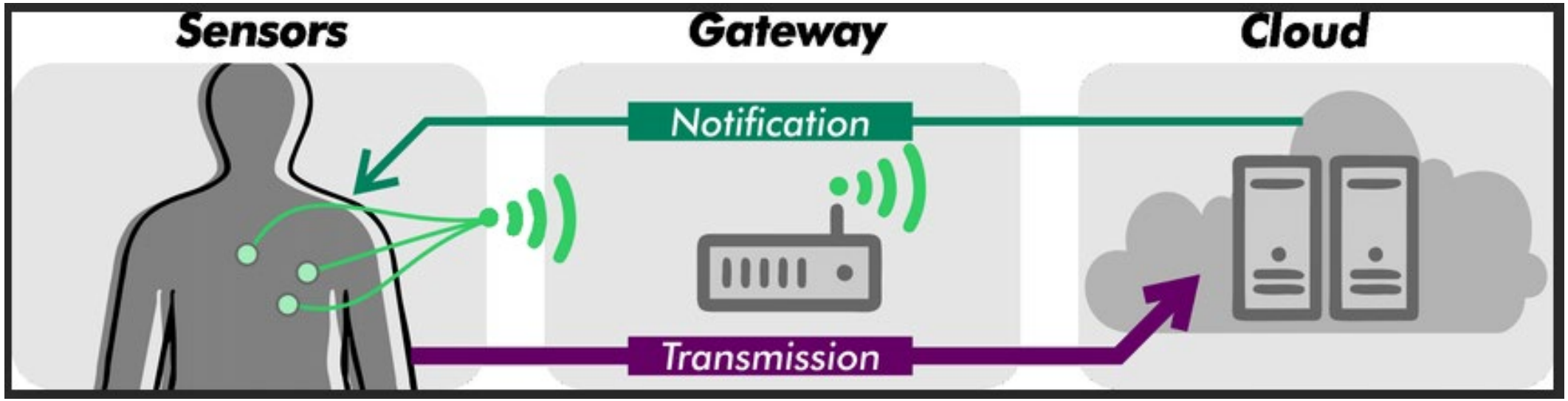


IOT REMOTE CONTROL EXAMPLES



IOT HAS NO LOCATION OR DISTANCE LIMITS

- In IoT architecture, there is (theoretically) no limitation of location or distance between two or more devices
  - Devices and components can be spread across the globe
  - There is, however, a practical consideration regarding bandwidth availability and latency



IOT COMMUNICATION

- IoT connectivity can be:
  - Wired or wireless, using just about any network transmission type
- Device-to-Device
  - Direct communication between two devices
- Device-to-Cloud
  - Communicates directly to a cloud service
- Device-to-Gateway
  - Communicates to a centralized gateway that gathers data and then sends it to an application server based in the cloud
- Back-End Data Sharing
  - Scale devices to a cloud model
  - Allows for multiple devices to interact with one or more application servers

IOT NETWORK SCOPES

- PAN
  - IoT wearables + Smartphone
- LAN
  - IoT Wi-Fi Devices
- WAN
  - IoT Long Range Devices

IOT COMMUNICATION PROTOCOLS AND OSES

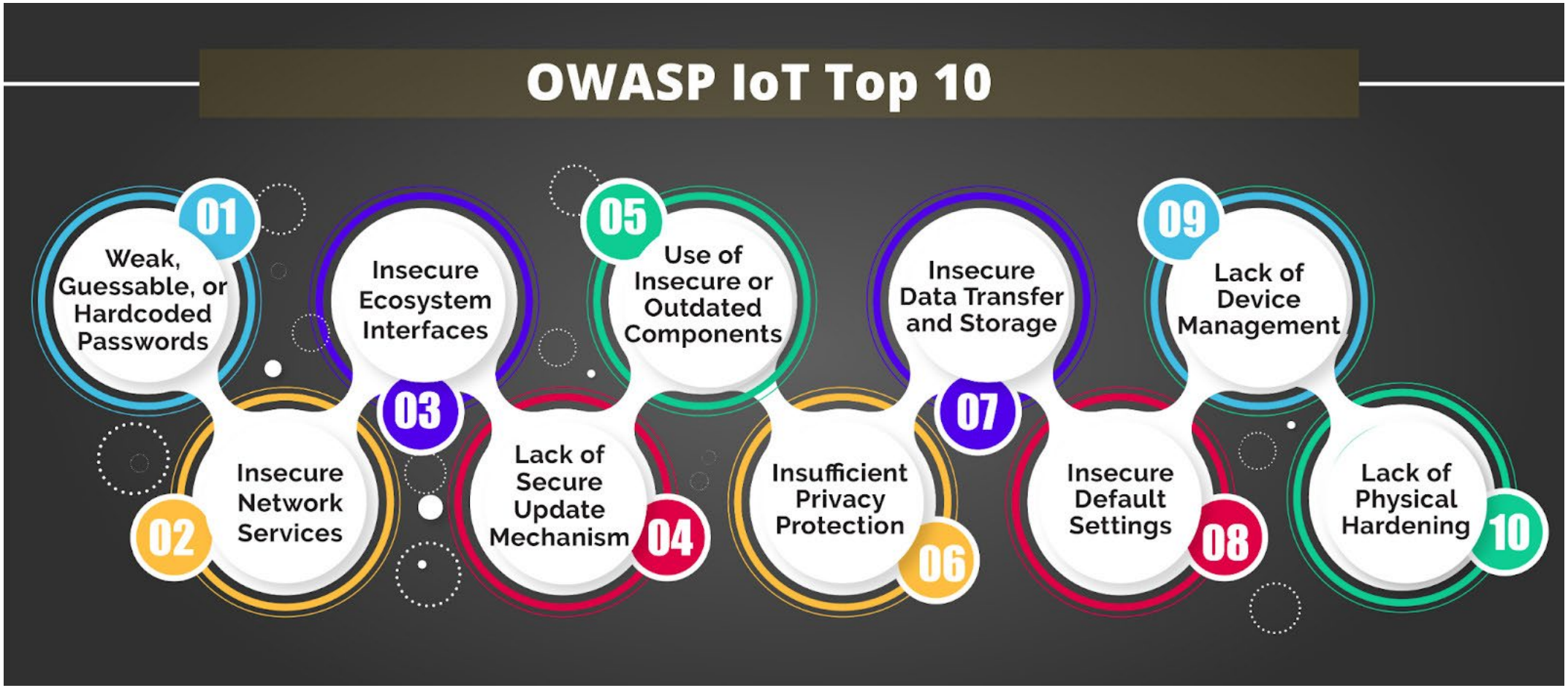
Short-Range Wireless Communications	Medium-Range Wireless Communications	Long-Range Wireless Communications	Wired Communications	IoT Operating Systems

• Bluetooth Low Energy (BLE)
• Light-Fidelity (Li-Fi)
• NFC
• QR Codes/ Barcodes
• RFID
• Thread
• Wi-Fi
• Wi-Fi Direct
• Z-Wave
• ZigBee
• ANT
	• Ha-Low
	• LTE-Advanced
	• 6LoWPAN
	• QUIC
		• Low-power WAN (LPWAN)
		  • LoRaWAN
		  • Sigfox
		  • Neul
		• Very Small Aperture Terminal (VSAT)
		• Cellular
			• Ethernet
			• Multimedia over Coax
			• Power-line Communication (PLC)
				• RIOT OS
				• ARM embedded OS
				• RealSense OS X
				• Nucleus RTOS
				• Brillo
				• Contiki
				• Zephyr
				• Ubuntu Core
				• Integrity RTOS
				• Apache Mynewt
				• Windows 10 IoT Core

18.3 IOT VULNERABILITIES AND THREATS

- OWASP Top 10
- IoT Threats

IOT VULNERABILITIES



OWASP TOP 10 IOT VULNERABILITIES

1. Weak, guessable, or hardcoded passwords
   - Use of easily brute-forced, publicly available, or unchangeable credentials
   - Includes backdoors in firmware or client software that grants unauthorized access to deployed systems
2. Insecure network services
   - Unneeded or insecure network services running on the device itself, especially those exposed to the internet
   - Compromises the confidentiality, integrity/authenticity, or availability of information or allows unauthorized remote control
3. Insecure ecosystem interfaces
   - Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device
   - Allows compromise of the device or its related components
   - Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering

OWASP TOP 10 IOT VULNERABILITIES (CONT'D)

4. Lack of secure update mechanism
   - Lack of ability to securely update the device
   - Includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit)
   - Lack of anti-rollback mechanisms
   - Lack of notifications of security changes due to updates
5. Use of insecure or outdated components
   - Use of deprecated or insecure software components/libraries that could allow the device to be compromised
   - This includes insecure customization of operating system platforms
   - The use of third-party softwar or hardware components from a compromised supply chain
6. Insufficient privacy protection
   - User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

OWASP TOP 10 IOT VULNERABILITIES (CONT'D)

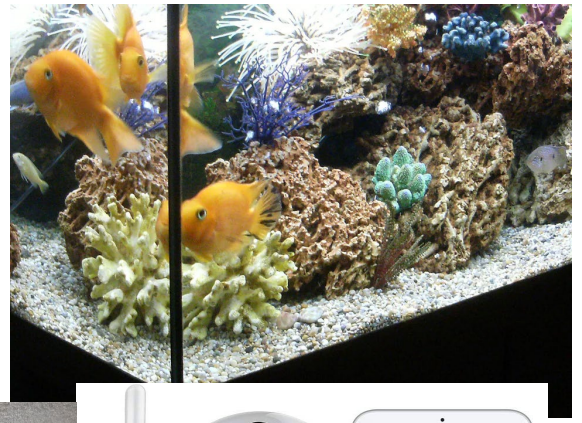
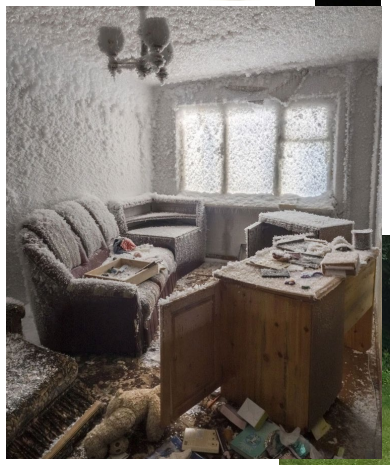
7. Insecure data transfer and storage
   - Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8. Lack of device management
   - Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9. Insecure default settings
   - Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
10. Lack of physical hardening
    - Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

IOT THREATS

- Common Threats

IOT PROVIDES ENDLESS ATTACK OPPORTUNITIES

- Casino lobby smart aquarium
  - Used as pivot to steal 10 GB of high roller data
- My Friend Cayla Bluetooth-enabled interactive doll
  - Attackers take over its camera, mic, and speaker
  - Banned in Germany after high-profile incidents
- DDoS takes down home thermostats
  - Mirai botnet leaves residents without heat
  - 2 apt. complexes, 2 weeks, freezing weather
- Baby monitor remote takeover
  - Attacker moves camera/views and speaks to child
  - 9 models reported from 2009 - 2022
- Jeep SUV remote control hijack
  - Weak password in firmware update
  - Made it speed up, slow down, and veer off the road

COMMON IOT THREATS

- DDoS
  - Devices join a botnet to perform DDoS against other targets
- Exploiting HVAC
  - Attacker uses shodan.io to find targets, then uses www.defpass.com to find default credentials
  - If the attacker can log in, they can send unauthorized commands to the HVAC system, possibly also breaching an IT network
    - Even though it is air-gapped from the IoT network
    - Uses environmental (temperature) changes to indicate binary data
- Rolling code
  - Used to steal cars; The ability to jam a key fob's communications to the car, sniff the fob's code and then create a subsequent code
  - Attacker uses rfcat-rolljam or RFCrack to perform the attack
- BlueBorne Attack
  - Attacks against Bluetooth devices

COMMON IOT THREATS (CONT'D)

- Jamming
  - Jams the signal between sender and receiver
- Remote Access using Backdoor
  - Attacker turns the IoT device into a backdoor to gain access into an organization's network
- Remote Access using Telnet
  - Obtain information shared between connected devices including hardware and software versions
- Rootkits/Exploit kits
  - Malicious script exploits poorly patched vulnerabilities in an IoT device
- MITM
  - Attacker pretends to be a legitimate sender
  - Intercepts and hijacks all communication between sender and receiver

COMMON IOT THREATS (CONT'D)

- Replay
  - Attacker intercepts legitimate messages
  - Continuously resends the message to the target device to crash it or its service
- Forged malicious devices
  - Attacker replaces authentic IoT devices with malicious ones
  - Requires physical access to the network
- Side channel attack
  - Attacker observes the emission of signals (side-channels) to obtain information about encryption keys
- Sybil attack
  - Attacker uses multiple forged identities to create the strong illusion of roadway traffic congestion
  - Affects communication between neighboring nodes and the network
  - Creates chaos and safety risks

COMMON IOT THREATS (CONT'D)

- Client Impersonation
  - Attacker masquerades as a legitimate smart device/server
  - Performs unauthorized activities or accesses sensitive data
- SQL Injection
  - Attacker performs SQL injection against vulnerable web or mobile apps
  - Gains access to the device or back end data
- Software-Defined Radio (SDR) Attack
  - Attacker uses a software-based radio to examine communication signals passing through an IoT network
  - Can send spam messages to interconnected devices

COMMON IOT THREATS (CONT'D)

- Fault Injection Attack
  - An attacker tries to introduce fault behavior in an IoT device
    - Exceeds operating temperature, voltage, frequency, etc.
  - Seeks to exploit faults to compromise device security
- Network Pivoting
  - Attacker uses a malicious smart device to connect and gain access to a closed server
  - Uses that connection as a entry point to attack other normally-unreachable devices
- DNS Rebinding Attack
  - Used to breach a private network by causing the victim's web browser to access computers at private IP addresses and return the results to the attacker

HOW AN ATTACKER PROFITS FROM A COMPROMISED IOT DEVICE

- Creates a botnet for use or rent
- Sells compromised data
- Performs malicious activities
- Demands a ransom to unlock devices
- Uses the device to steal a victim's identity, credit card information, or other data
- Uses compromised CCTV cameras and baby monitors to snoop on or terrorize families

SCENARIO

- You are attending a cybersecurity conference and just watched a security researcher demonstrating the exploitation of a web interface on a SCADA/ICS component.
- This caused the device to malfunction and be destroyed.
- You recognize that the same component is used throughout your company's manufacturing plants.
- What can be done to protect against this emergent threat?
- **Evaluate if the web interface must remain open for the system to function**
  - **If it isn't needed, block the web interface**

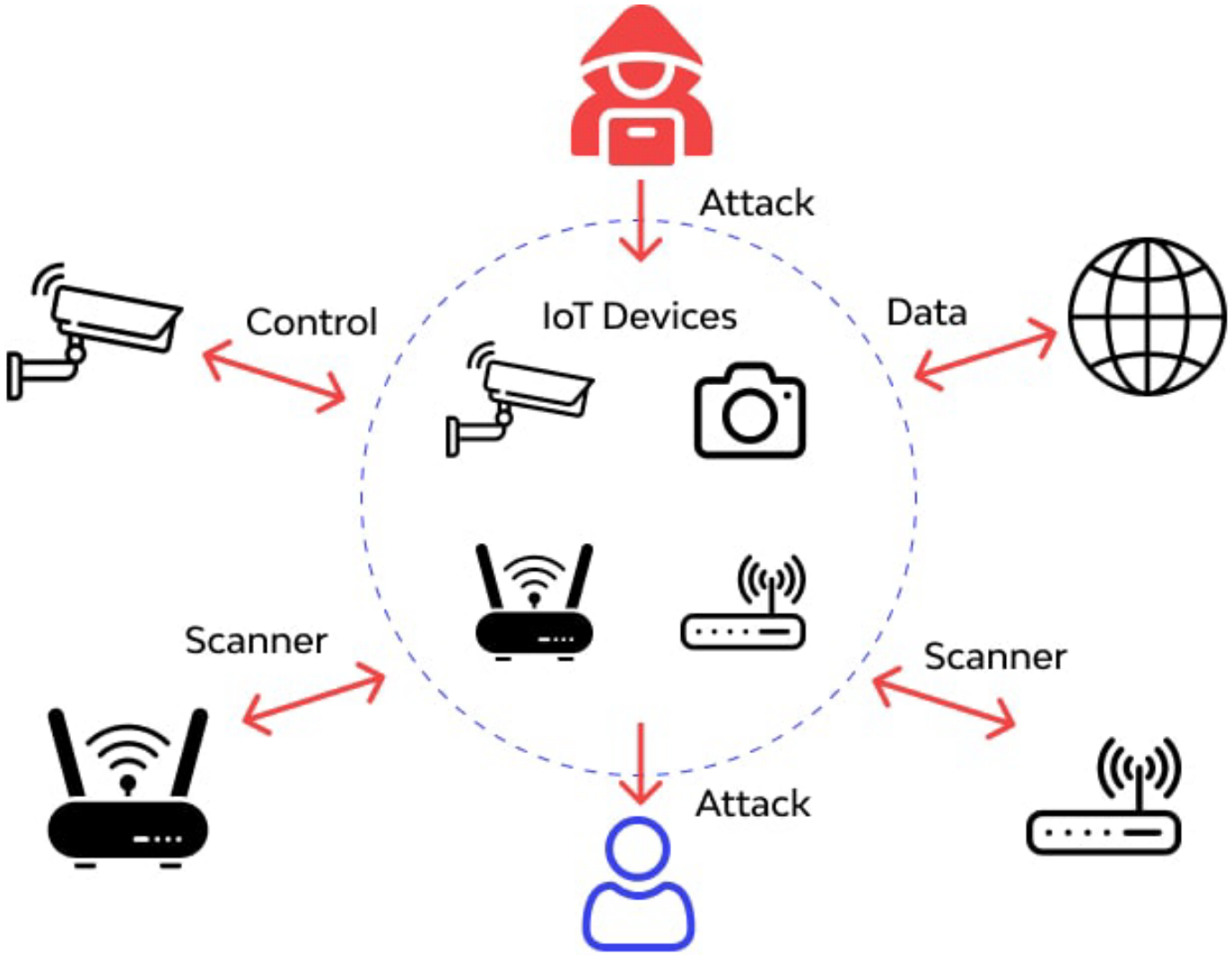
SCENARIO EXPLAINED

- The most immediate protection against this emergent threat would be to block the web interface from being accessible over the network
- Before doing this, you must evaluate whether the interface needs to remain open for the system to function properly
- If it is not needed, you should block it to minimize the SCADA/ICS component's attack surface
- Ideally, your SCADA/ICS components should already be logically or physically isolated from the enterprise network

18.4 IOT HACKING METHODOLOGY AND TOOLS

- Methodology
- Reconnaissance and Scanning

ATTACKING IOT



IOT HACKING METHODOLOGY

1. Take time to familiarize yourself with IoT technologies:
   - Architecture
   - Hardware
   - Physical interfaces
   - Signaling
   - Network protocols
   - Device-specific operations
2. Follow general hacking steps of reconnaissance, penetration and control
   - Keep in mind that there are many, many variations in IoT devices
   - Consider narrowing your focus to just a few IoT device types and use cases
3. Expand attack approaches to include:
   - Physical/environmental attacks
   - Device-specific hardware and software
   - Network communications
   - Control instructions and management apps
   - Cloud Services

IOT HARDWARE ANALYSIS

- Basic Tools
- Specialized Tools

BASIC HARDWARE TOOLS

- Soldering Equipment
  - Attach and detach hardware components to circuit boards; physically change circuit pathways
- Microscope/magnifying glass
  - Help improve soldering or tiny part handling precision
- Communication Interface (such as a JTAG)
  - Connect to and communicate with ICS devices
- Screwdrivers/tweezers
  - Open or disassemble devices, move jumpers and connections

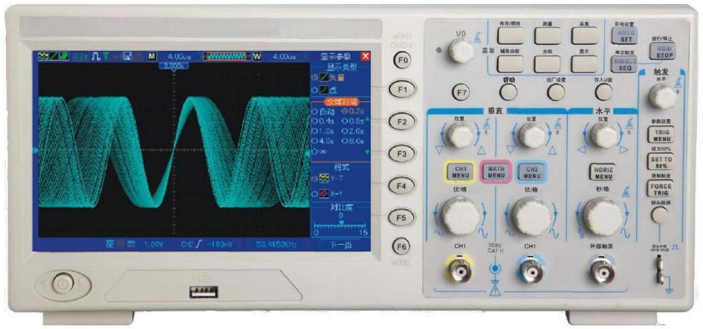
BASIC HARDWARE TOOLS (CONT'D)

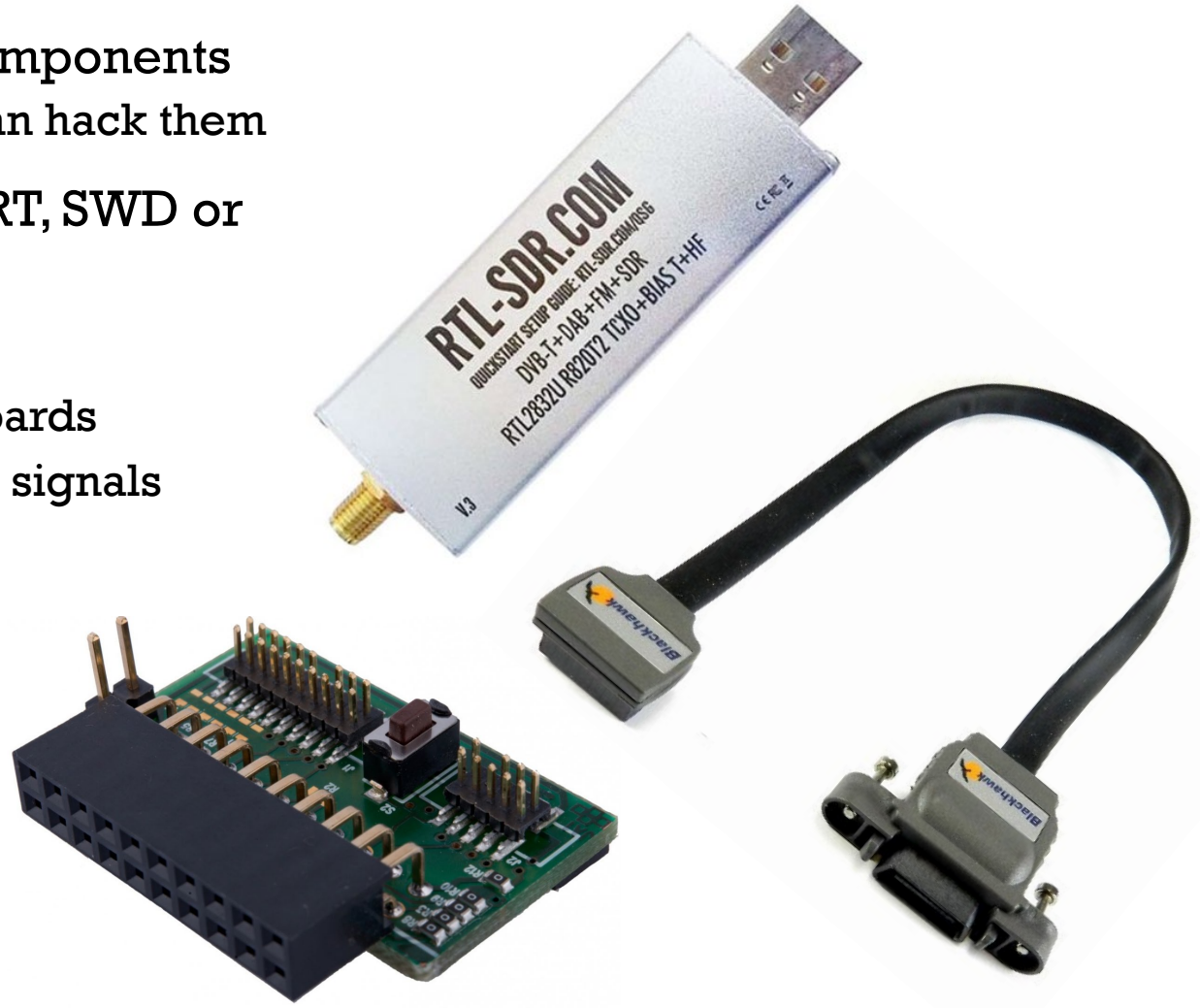
- Signal Analyzer
  - Test the operation of chip pins
- Multimeter
  - Test circuit voltage, current, resistance/continuity
- Memory Programmer
  - Use to reprogram flash memory, EPROMs/EEPROMs
- Oscilloscope
  - Visually interpret analog and digital signals

EPROM MEMORY PROGRAMMER KIT EXAMPLE

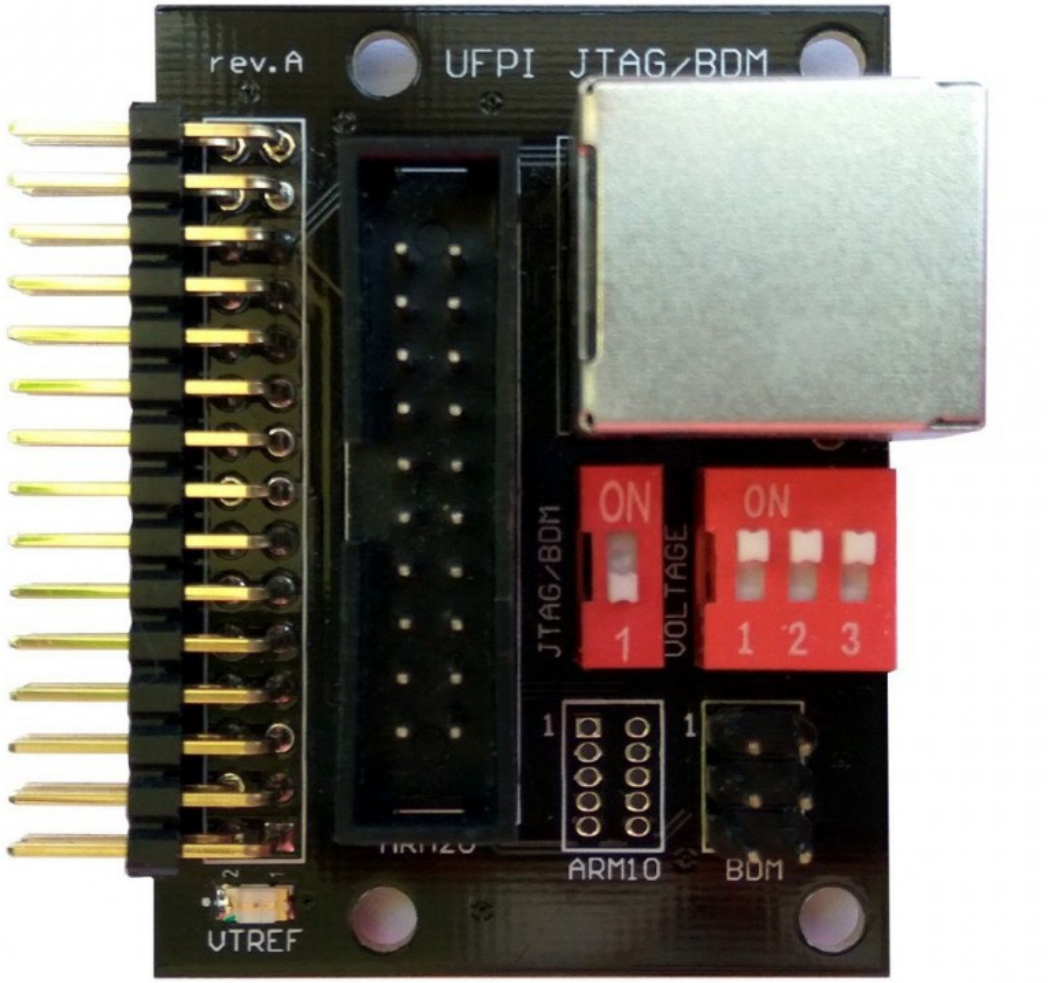
HARDWARE ANALYSIS

- Evaluate physical and hardware components
  - Understand how they work so you can hack them
- See if you can connect to JTAG, UART, SWD or USB interfaces
- Use tools like:
  - JTAG Dongle to connect to circuit boards
  - Digital Storage Oscilloscope to view signals
  - RF analyzers
  - Firmware analyzers



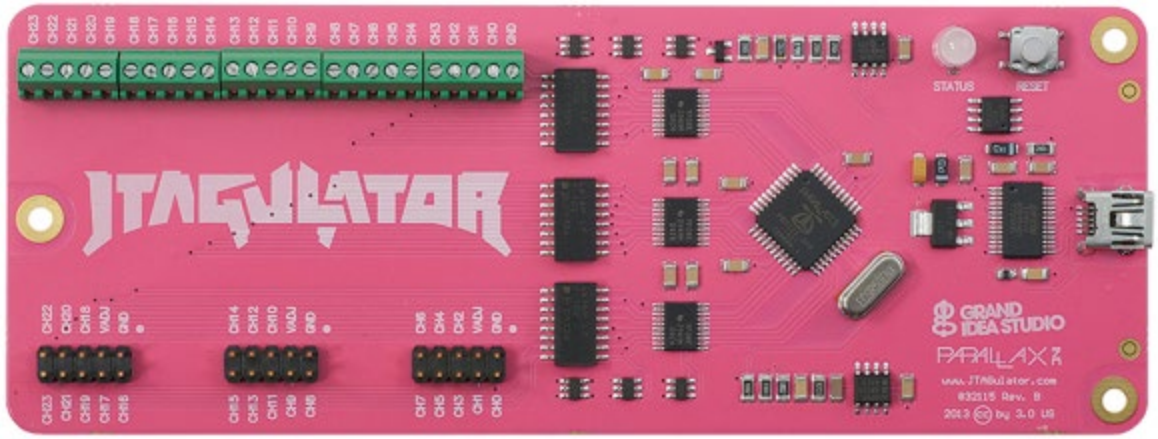


JTAG EXAMPLE



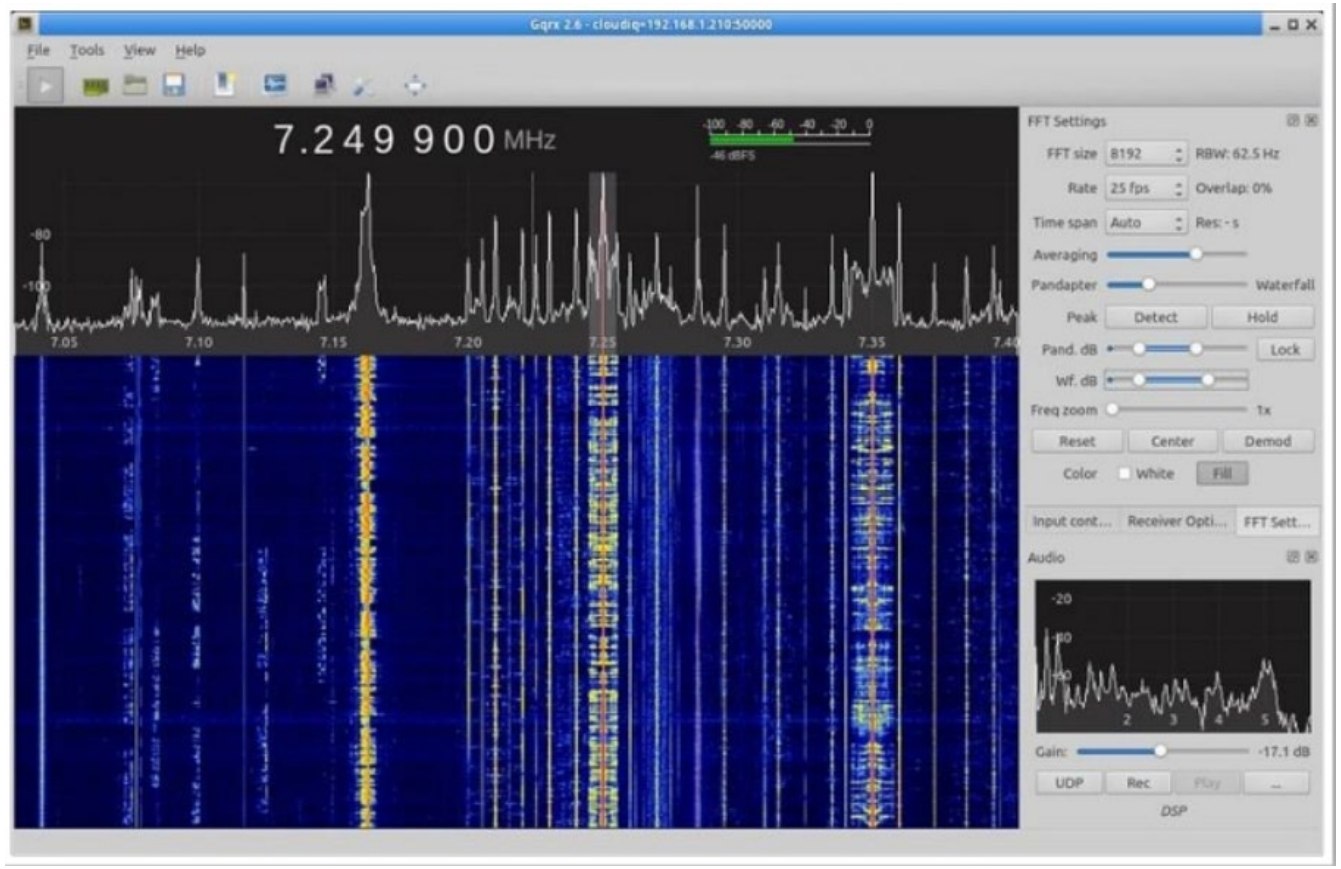
JTAGULATOR

- Open source hardware hacking tool
- Used to identify on-chip debug (OCD) interfaces on unfamiliar hardware
- Provides chip-level control of a target device
  - Extract program code or data, modify memory contents, or affect device operation on-the-fly



IOT SPECTRUM ANALYSIS EXAMPLE

- Use dongles such as:
  - FunCube
  - Airspy
  - HackRF
  - RTL-SDR
- Along with:
  - Gqrx spectrum analyzer

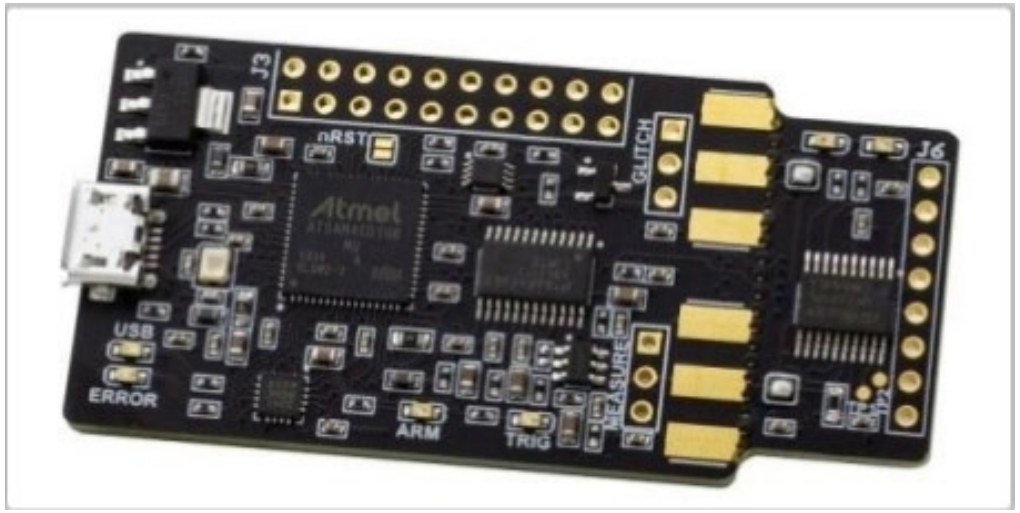


FIRMWARE AND OS ANALYSIS

- See if the firmware is cryptographically signed, and has an update mechanism
- Use tools such as:
  - IoTInspector
  - Binwalk
  - Firmware Mod Kit
  - Firmware Analysis Toolkit
  - Firmalyzer Enterprise

CHIP WHISPERER NANO FAULT INJECTOR

- Inject glitches into any embedded hardware
- Gain access to the clock or input power of the device



DEBUGGERS / DISASSEMBLERS

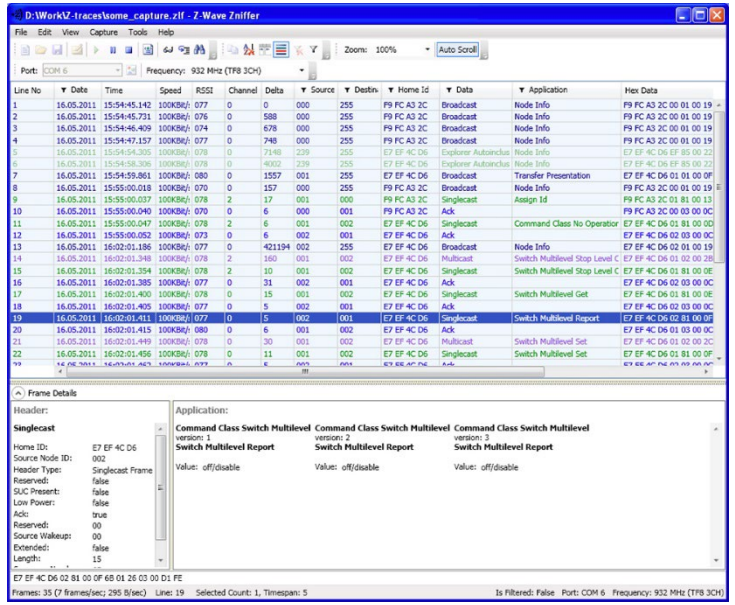
- GDB
  - Linux debugger attackers can use to understand the process of on-chip executions
- OpenOCD
  - Allows attackers to remote to the chip they want to examine using Gnu Project Debugger (TCP 333) or Telnet (TCP 23)
- Binwalk
  - Scan and examine firmware binaries and images
- Fritzing
  - Assists attackers in designing electronic diagrams and circuits
- Radare2
  - Portable framework to analyze and reverse engineer binaries
- OllyDbg, IDA Pro
  - A code-disassembling tool to examine binaries

IOT RECON

- OSINT
- Sniffing
- Scanning

IOT DEVICE RECONNAISSANCE TOOLS

- Shodan.io
- Censys.io
- Thingful.net
- Google Dorks
- Z-Wave Sniffer
- CloudShark protocol analyzer
- Ubiqua Protocol Analyzer
- Wireshark
- Multiping
- Nmap



NMAP IOT DEVICE SCANNING

- Scan TCP ports of a specific device:

```
nmap -n -Pn -sS -pT:0-65535 -v -A -oX <target>
```

- Scan TCP and UDP ports of a specific device:

```
nmap -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <target>
```

- Scan using IPv6:

```
nmap -6 -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <target>
```

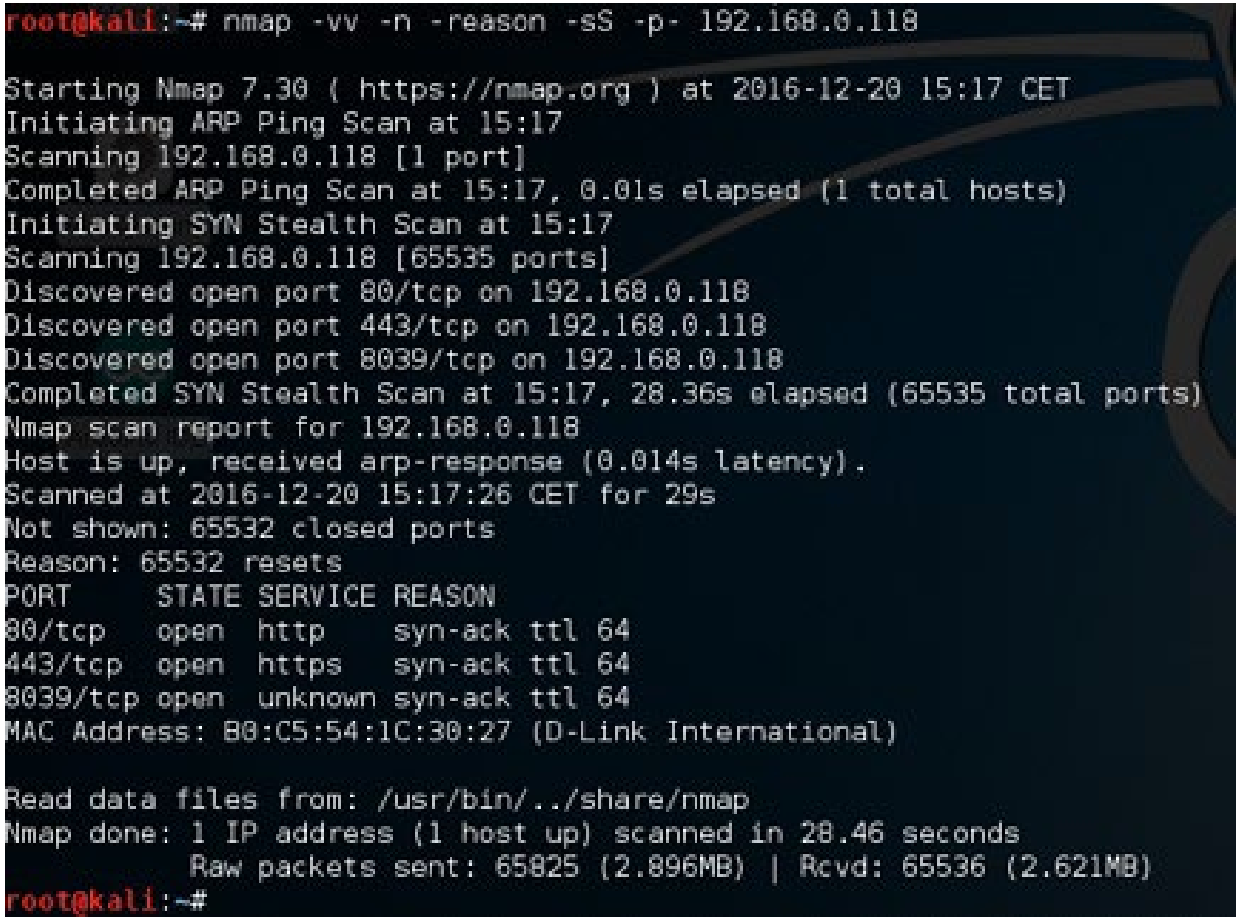
SCAN FOR DEVICES WITH DEFAULT CREDENTIALS

- Use IoTSeeker to scan a network:
  - Searches for specific IoT device types
  - Checks to see if the devices are using default, factory set credentials
  - Available on GitHub

```
/Users/rapid7/freetools>perl iotScanner.pl 1.23.123.431,
1.23.123.443,1.23.123.453,1.23.123.457,1.23.123.459,1.23.123.461,1.
23.123.462,1.23.123.463,1.23.123.465,1.23.123.466,1.23.123.467,1.23
.123.469,1.23.123.472,1.23.123.473,1.23.123.475,1.23.123.477,1.23.1
23.479,1.23.123.480,1.23.123.481
[device 1.23.123.431 is of type Stardot still has default passwd
 device 1.23.123.443 is of type Arecont has changed passwd
 device 1.23.123.453 is of type American Dynamics has changed passwd
 device 1.23.123.457 is of type W-Box has changed passwd
 device 1.23.123.459 is of type Arecont has changed passwd
 device 1.23.123.461 is of type American Dynamics has changed passwd
 device 1.23.123.462 is of type W-Box has changed passwd
 device 1.23.123.463 is of type Arecont has changed passwd
 device 1.23.123.465 is of type American Dynamics has changed passwd
 device 1.23.123.466 is of type W-Box has changed passwd
 device 1.23.123.467 is of type Arecont has changed passwd
 device 1.23.123.469 is of type American Dynamics has changed passwd
 device 1.23.123.472 is of type W-Box has changed passwd
 device 1.23.123.473 is of type W-Box has changed passwd
 device 1.23.123.475 is of type W-Box has changed passwd
 device 1.23.123.477 is of type W-Box still has default passwd
 device 1.23.123.479 is of type Arecont has changed passwd
 device 1.23.123.480 is of type American Dynamics has changed passwd
 device 1.23.123.481 is of type American Dynamics has default passwd
```

IOT DEVICE VULNERABILITY SCANNERS

- Nmap
- Mulit-pingbeSTORM fuzzer
- Metasploit
- IoTsploit
- IoTSeeker
- Bitdefender Home Scanner
- Firmalyzer
- IoTInspector
- RIoT Vulnerability Scanner
- Foren6
  - 6LoWPAN passive sniffer/scanner

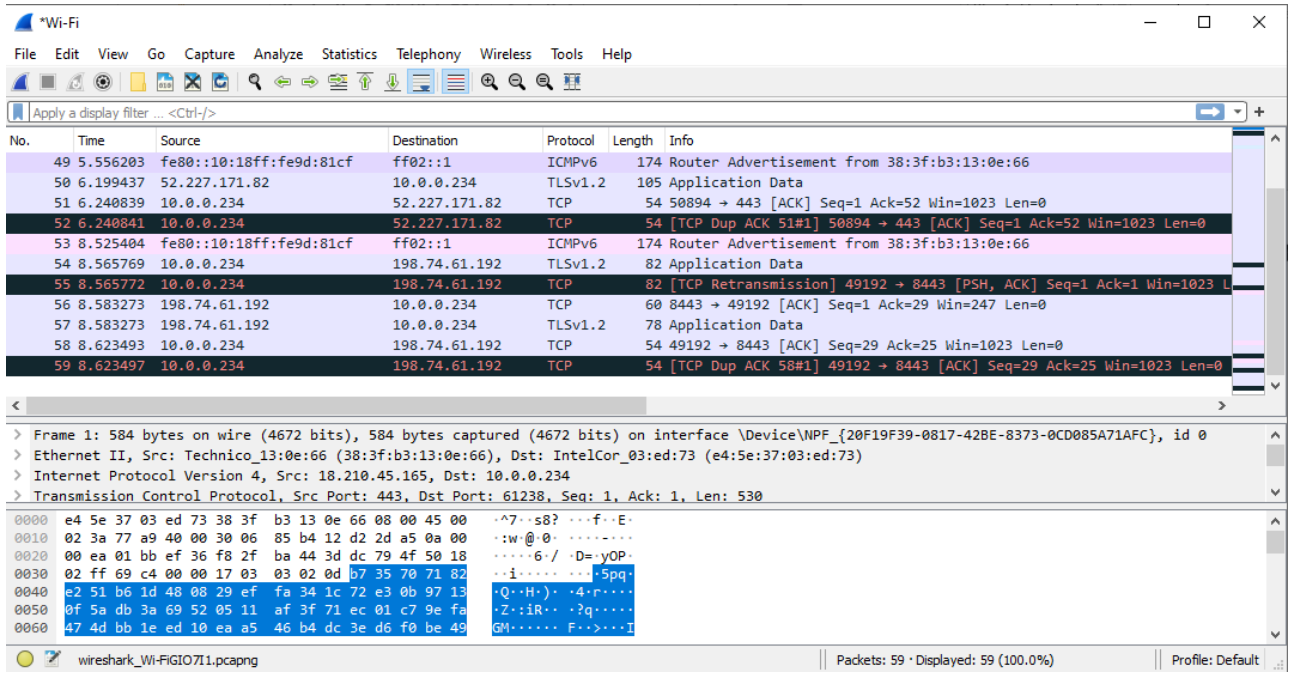


RETINA IOT (RIOT) VULNERABILITY SCANNER

- Identifies at-risk devices
- Pinpoints make and model
- Looks for open ports and backdoors, default credentials

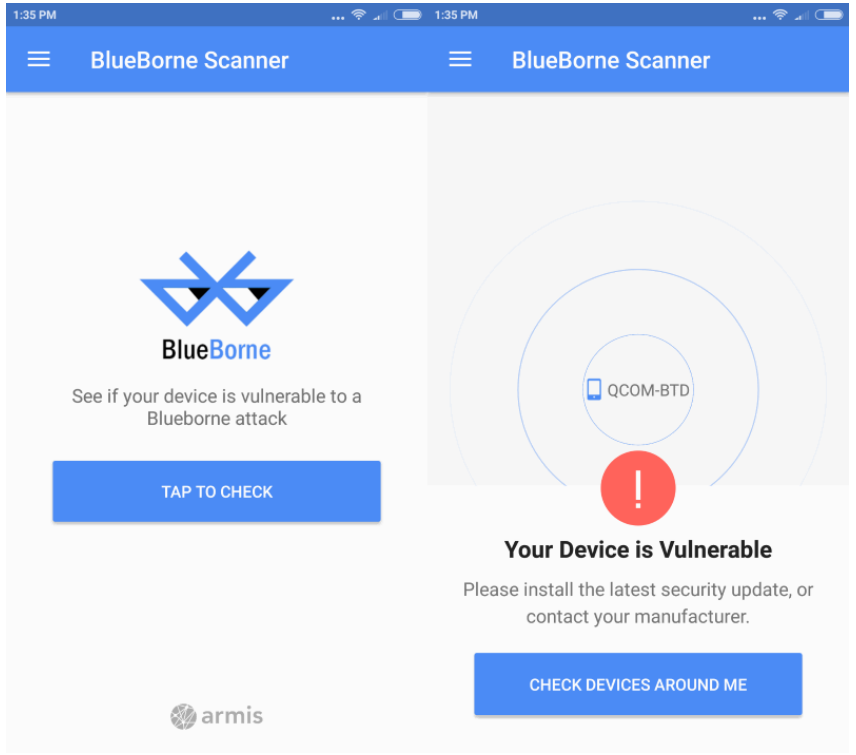
WIRELESS PROTOCOL TESTING

- Attempt to perform replay and MITM attacks
- Attempt to gain unauthorized network access
- See if you can connect using:
  - ZigBee
  - Bluetooth LE
  - 6LoWPAN
- Try to fuzz test the device
- Use tools such as:
  - Ubiqua Protocol Analyzer
  - Perytons Protocol Analyzer
  - Wireshark
  - SoapUI Pro
  - Attify Zigbee
  - Z3sec



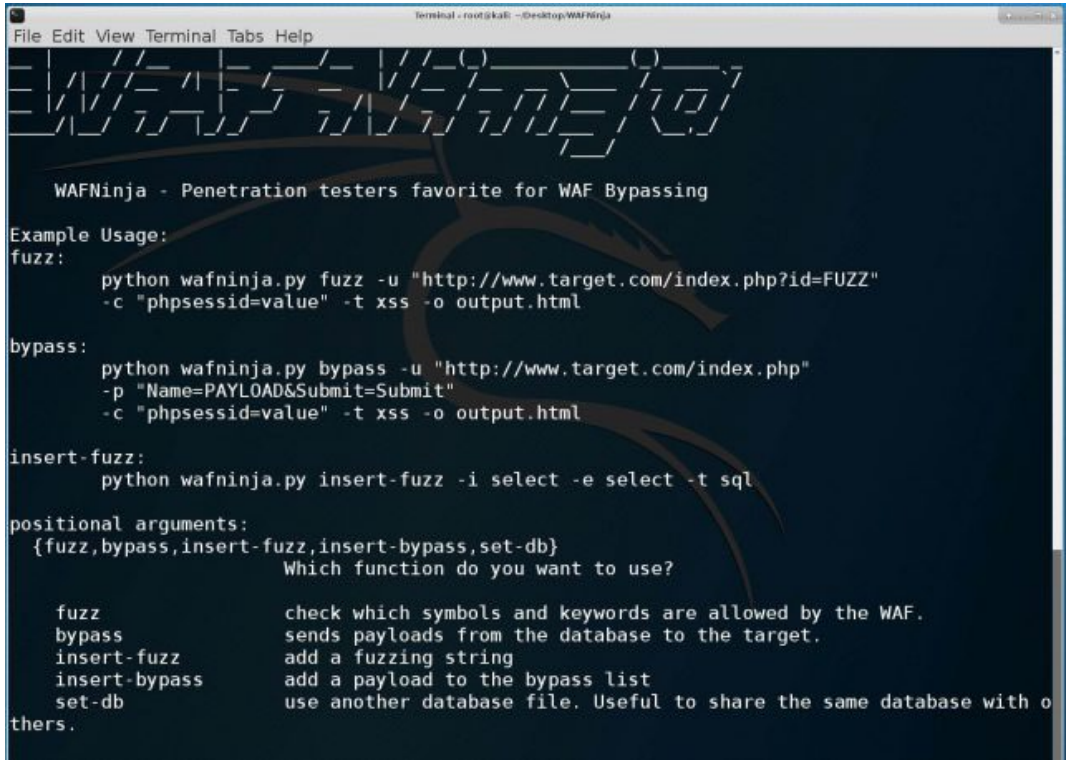
MOBILE APP TESTING

- Attempt to penetrate mobile apps that connect with the IoT device
- Try to access storage, and bypass authentication and authorization
- Use tools such as:
  - X-Ray
  - Threat Scan
  - Norton Halt exploit defender
  - Shellshock Scanner - Zimperium
  - Hackode
  - BlueBorne
  - EternalBlue Vulnerability Scanner



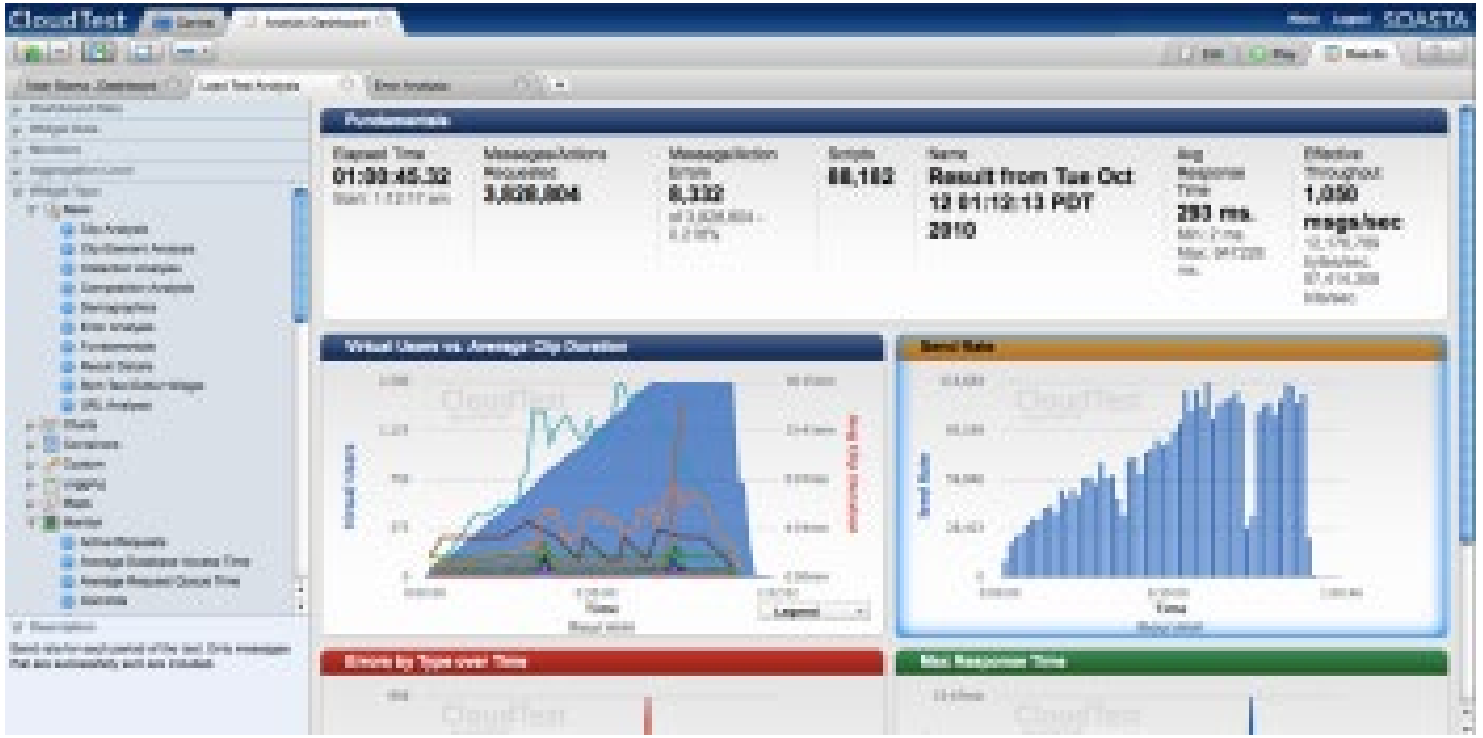
WEB APP TESTING

- Try typical attacks against a web app including buffer overflows, SQL injection, bypassing authentication, XSS/XSRF, code execution
- Use tools such as:
  - SAUCE LABS Functional Testing
  - PowerSploit
  - Kali Linux
  - WAFNinja
  - Arachni



CLOUD SERVICES TESTING

- Try to gain unauthorized access to cloud services for the IoT device
- Use tools such as:
  - ZEPHYR
  - SOASTA CloudTest
  - LoadStorm PRO
  - BlazeMeter
  - Nexpose

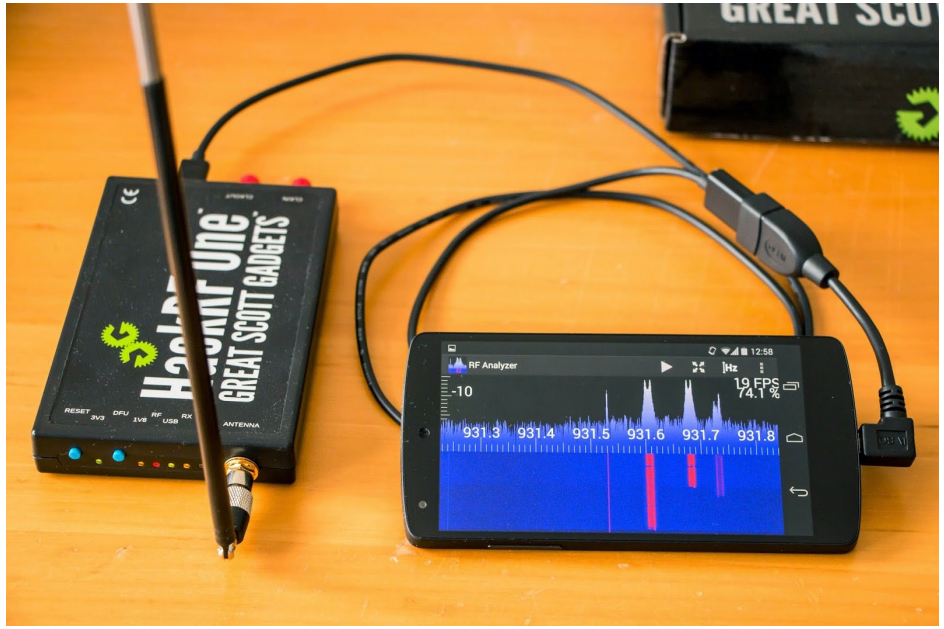


IOT ATTACKS

- Penetration and Control Tools

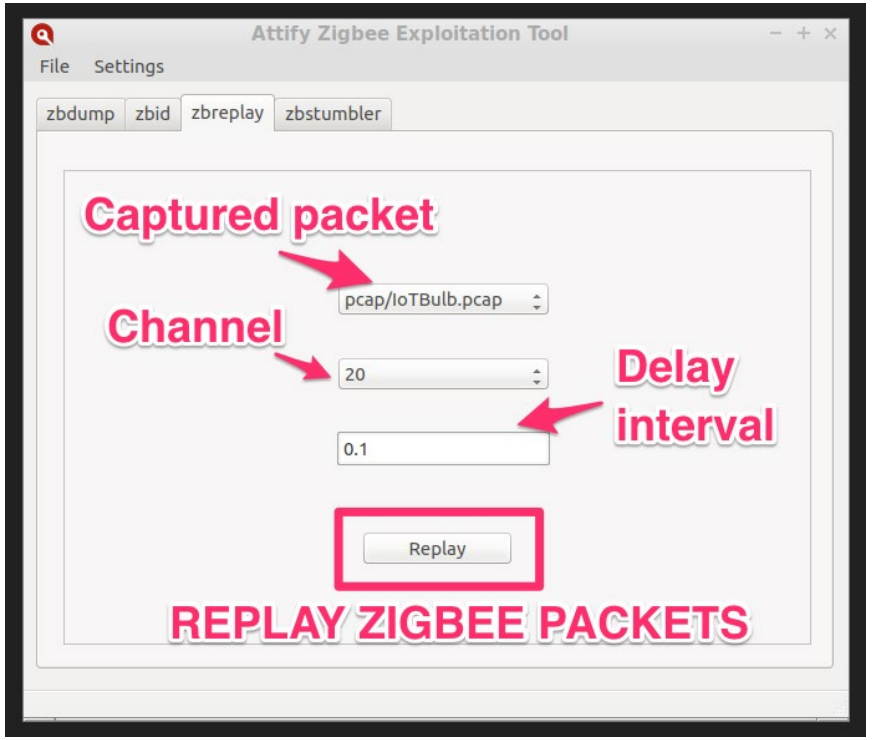
HACKRF ONE

- Software Defined Radio
- Can transmit or receive radio signals from 1 MHz to 6 GHz
- Can be used for:
  - Spectrum analysis
  - BlueBorne attack
  - Replay
  - Fuzzing
  - Jamming

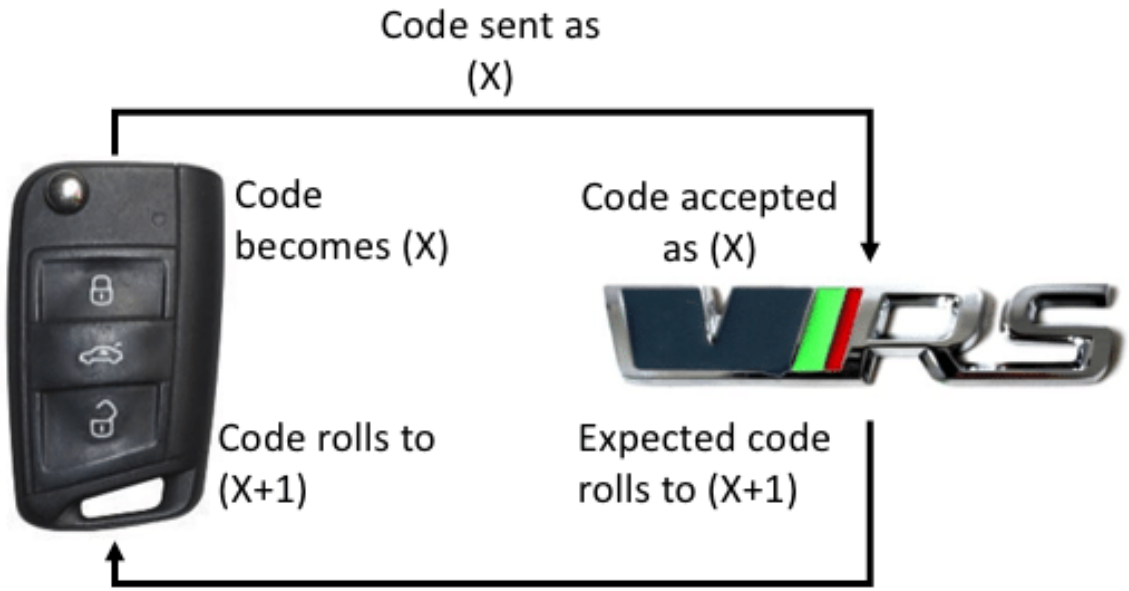


KILLERBEE AND ATTIFY ZIGBEE

- Attack Zigbee-enabled devices
  - Create an Atmel RzRaven USB Stick flashed with KillerBee
  - Install Attify Zigbee
  - Attack!
- KillerBee
  - Framework for Attacking ZigBee 802.15.4 networks
  - https://github.com/riverloopsec/killerbee
- Attify Zigbee Framework
  - GUI front end for RzRaven
  - https://github.com/attify/Attify-Zigbee-Framework

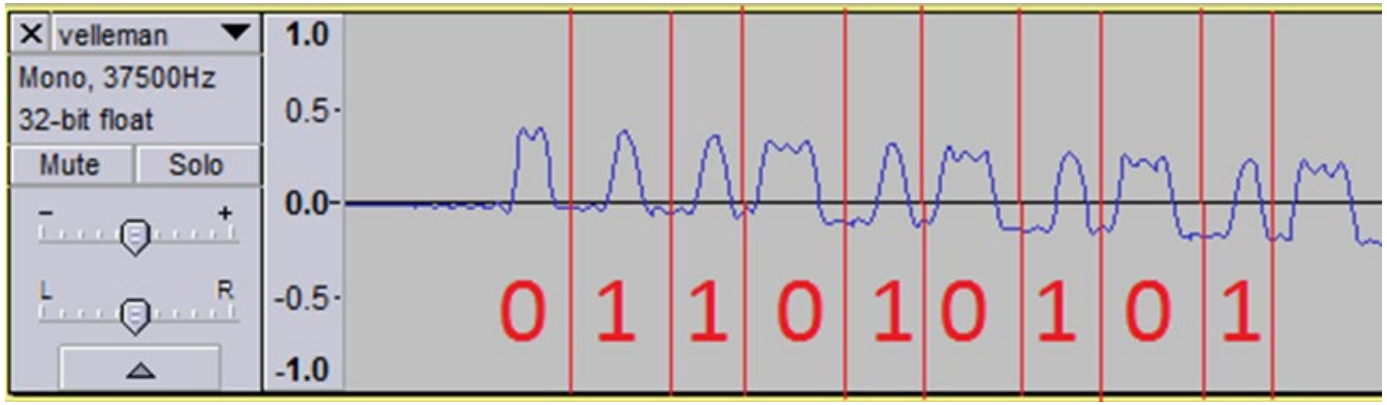


ROLLING CODE (ROLLJAM) ATTACK

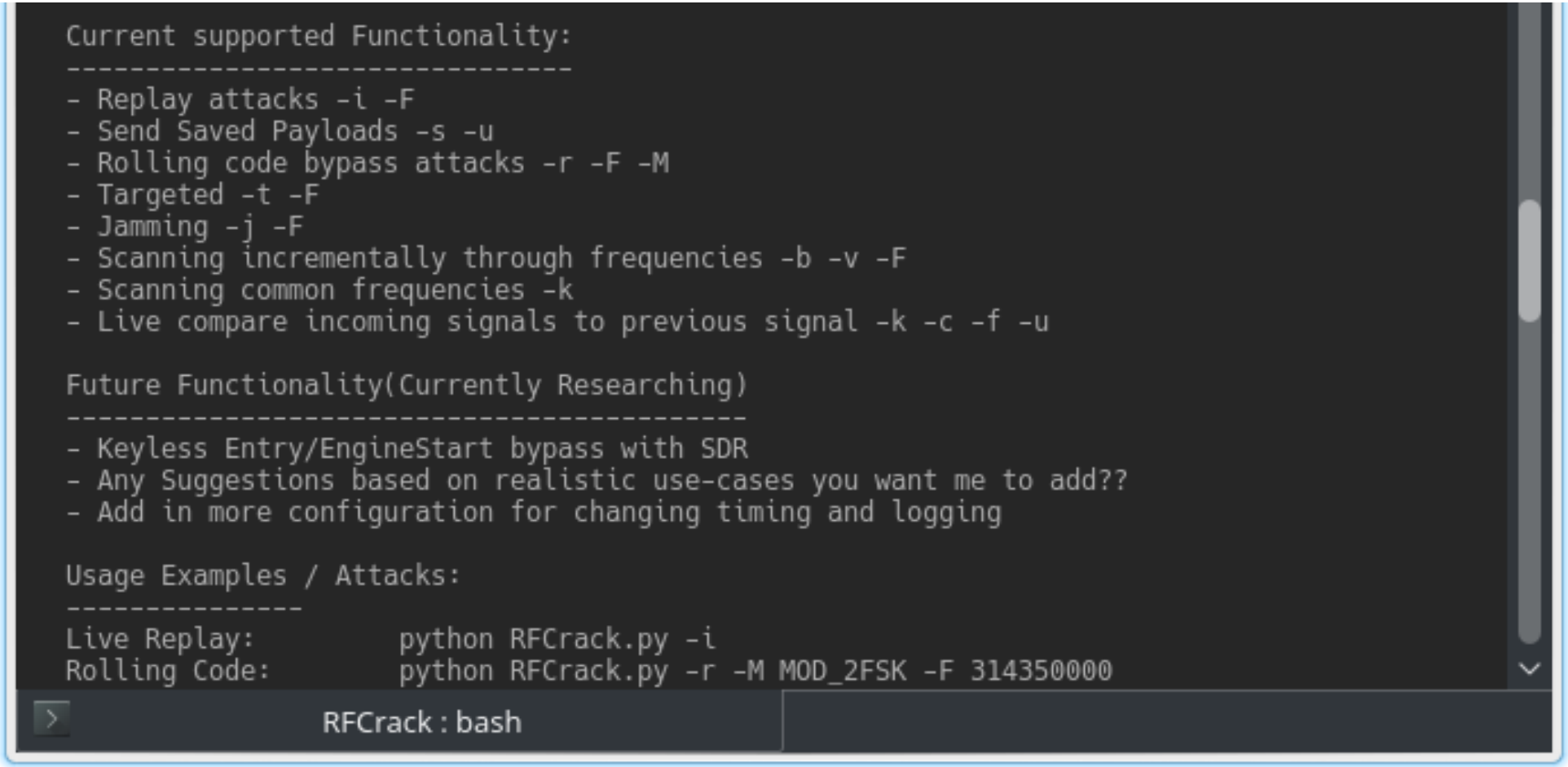


1. Capture code from the remote
2. Crack the code
3. Guess the next code
4. Transmit the code to the car

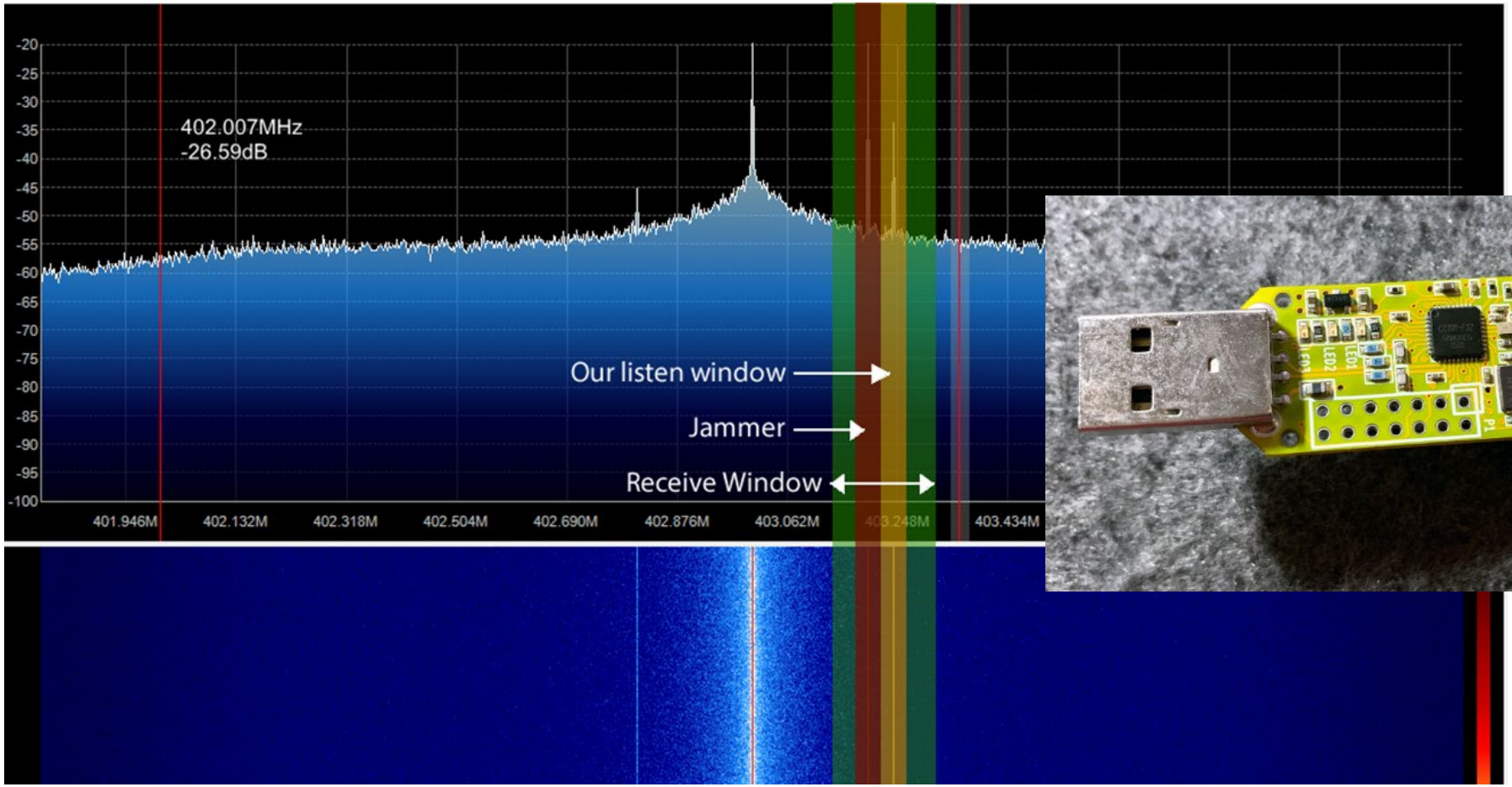
PROFIT!



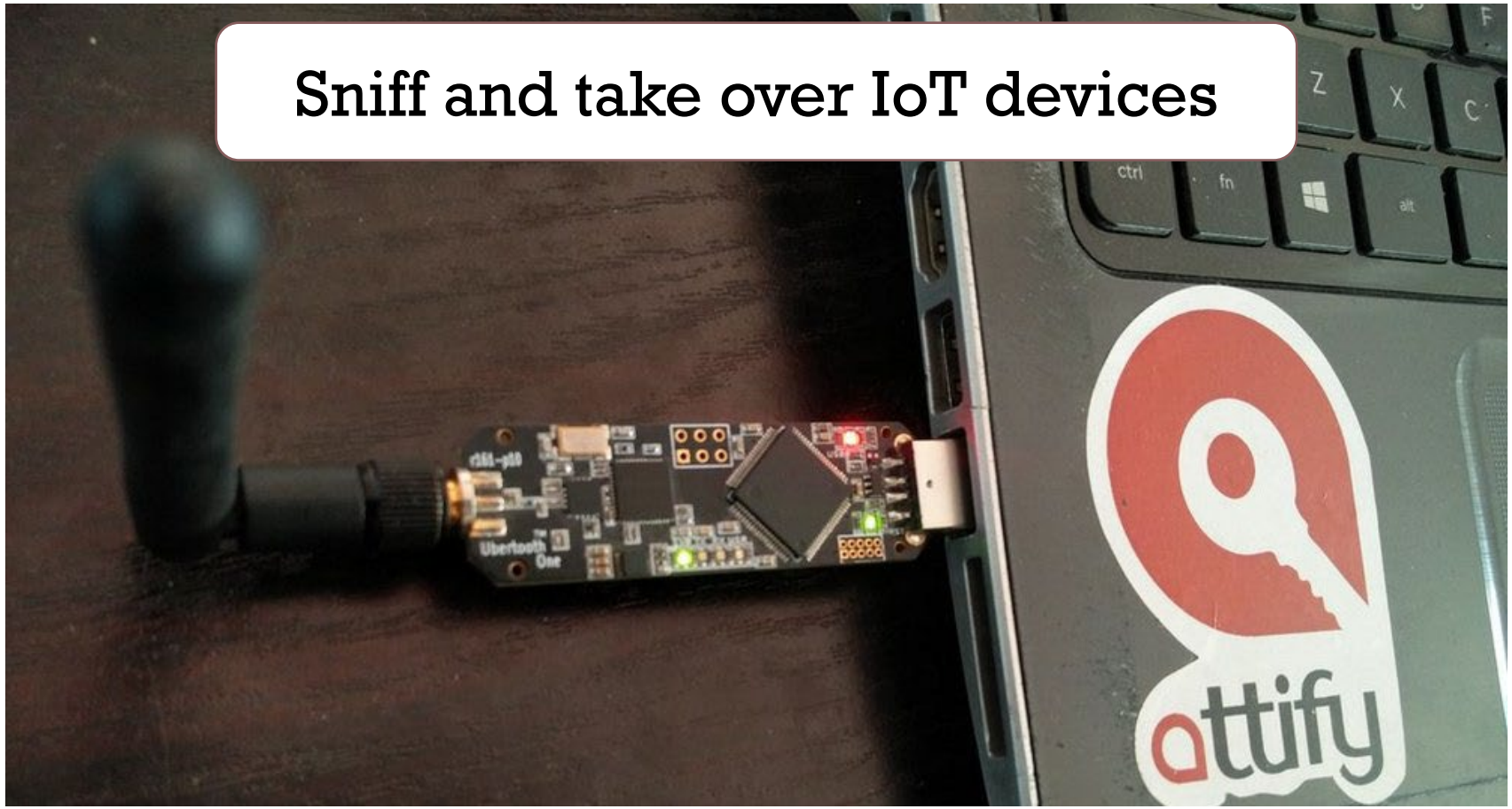
RFCRACK ROLLING CODE SOFTWARE



ROLLING CODE ATTACK EXAMPLE



GATTACKER IOT MITM EXAMPLE



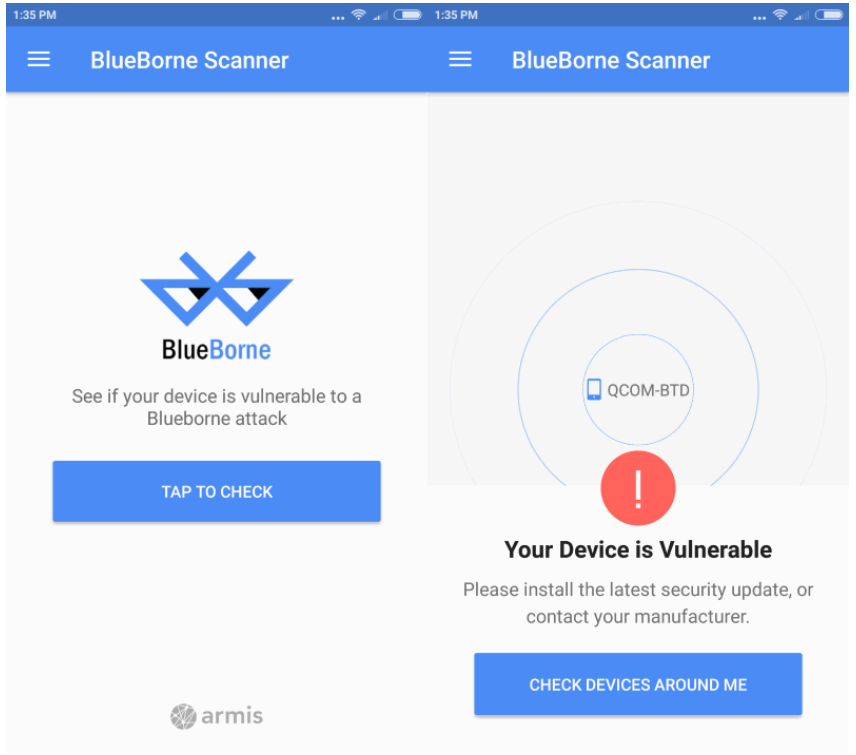
IOT REMOTE ACCESS ATTACKS

- Use Telnet to gain remote access
- Use Firmware Mod Kit to maintain access
- You can also compromise any system that normally has access to the device
  - Such as a smartphone

```
root@kali:/usr/share/firmware-mod-kit# ./extract-firmware.sh /root/docs/TechSegment/dd-wrt.v24_mi
cro_generic.bin
Firmware Mod Kit (extract) 0.99, (c)2011-2013 Craig Heffner, Jeremy Collake

Preparing tools ...
Scanning firmware...

Scan Time:     2013-06-17 16:55:46
Signatures:    193
Target File:   /root/docs/TechSegment/dd-wrt.v24_micro_generic.bin
MD5 Checksum:  4f9885b69026ac5d4225b6928e2e9c7d

DECIMAL       HEX             DESCRIPTION
--------------------------------------------------------------------------------
-----
0             0x0             TRX firmware header, little endian, header size: 28 bytes,  image
size: 1769472 bytes, CRC32: 0xE560D3A9 flags/version: 0x10000
28            0x1C            gzip compressed data, from Unix, NULL date: Wed Dec 31 19:00:00 1
969, max compression
2472          0x9A8           LZMA compressed data, properties: 0x6E, dictionary size: 2097152
bytes, uncompressed size: 2191360 bytes
670720        0xA3C00         Squashfs filesystem, little endian, DD-WRT signature, version 3.0
 size: 1095978 bytes,  525 inodes, blocksize: 131072 bytes, created: Fri Aug  6 21:19:38 2010

Extracting 670720 bytes of trx header image at offset 0
Extracting squashfs file system at offset 670720
Extracting squashfs files...
```

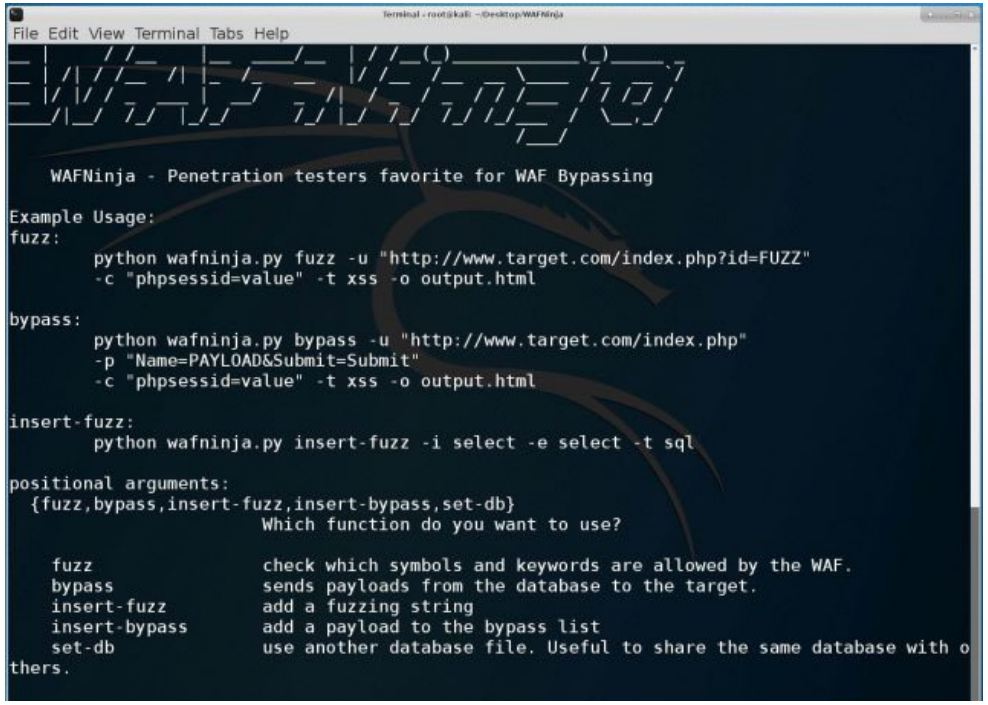
MOBILE APP ATTACKS

- Attempt to penetrate mobile apps that the IoT device connects to
- Try to access storage, and bypass authentication and authorization
- Use tools such as:
  - X-Ray
  - Threat Scan
  - Shellshock Scanner - Zimperium
  - Hackode
  - BlueBorne
  - EternalBlue Vulnerability Scanner



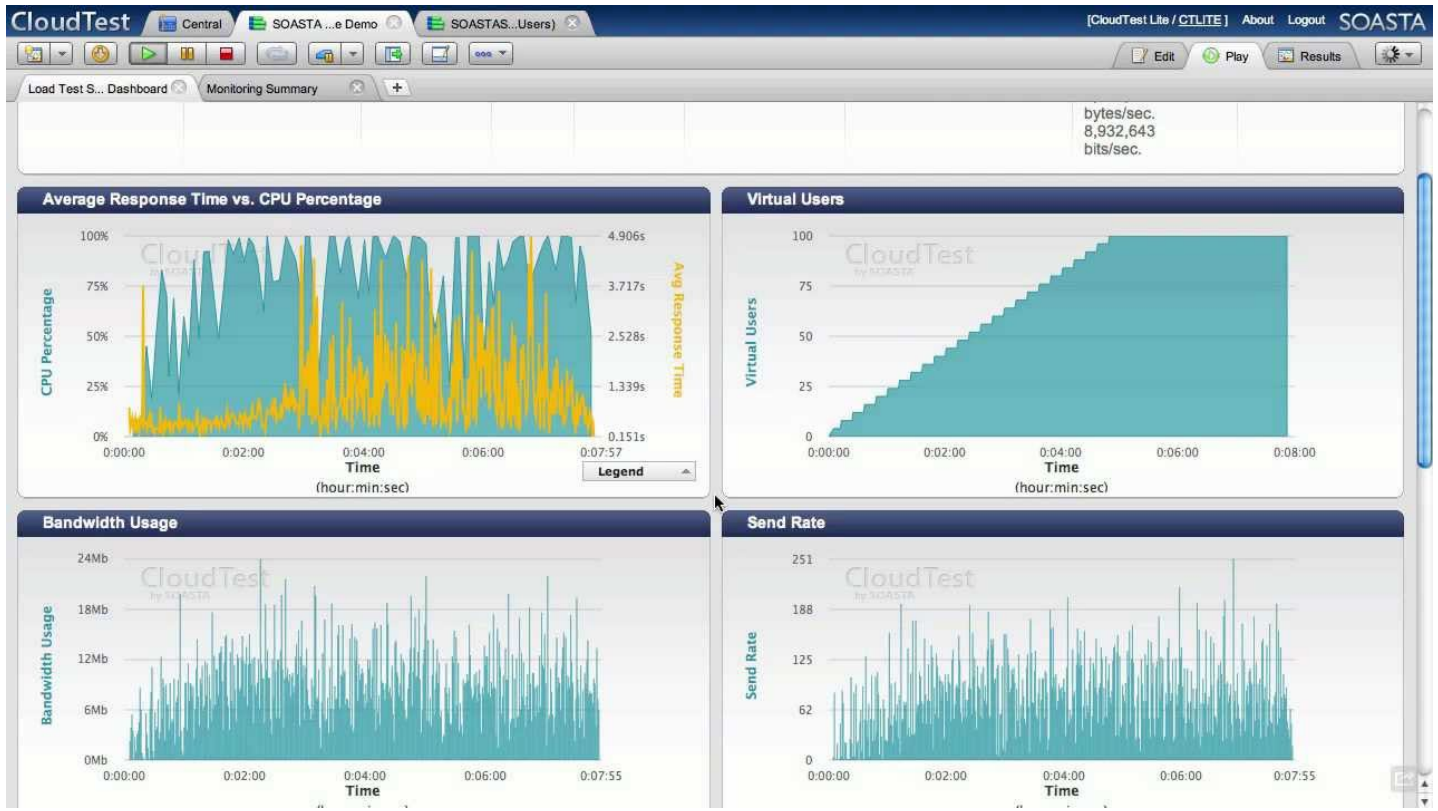
WEB APP ATTACKS

- Try typical attacks against a web app that aggregates/presents IoT data:
  - buffer overflows, SQL injection, bypassing authentication, XSS/XSRF, code execution, etc.
- Use tools such as:
  - SAUCE LABS Functional Testing
  - PowerSploit
  - Kali Linux
  - WAFNinja
  - Arachni



CLOUD SERVICES ATTACKS

- Try to gain unauthorized access to cloud services for the IoT device
- Use tools such as:
  - ZEPHYR
  - SOASTA CloudTest
  - LoadStorm PRO
  - BlazeMeter
  - Nexpose

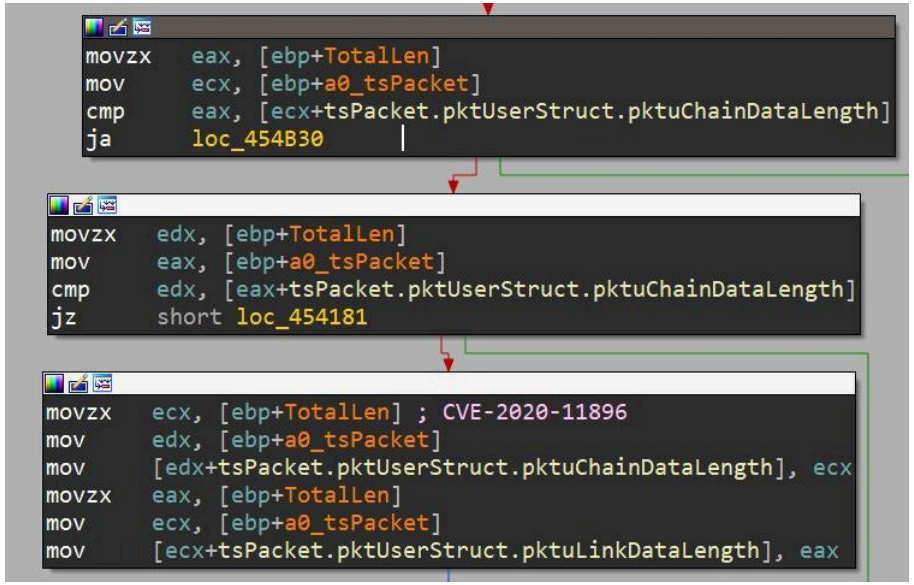


NOTABLE IOT ATTACKS

- Famous and Infamous Attacks

RIPPLE20

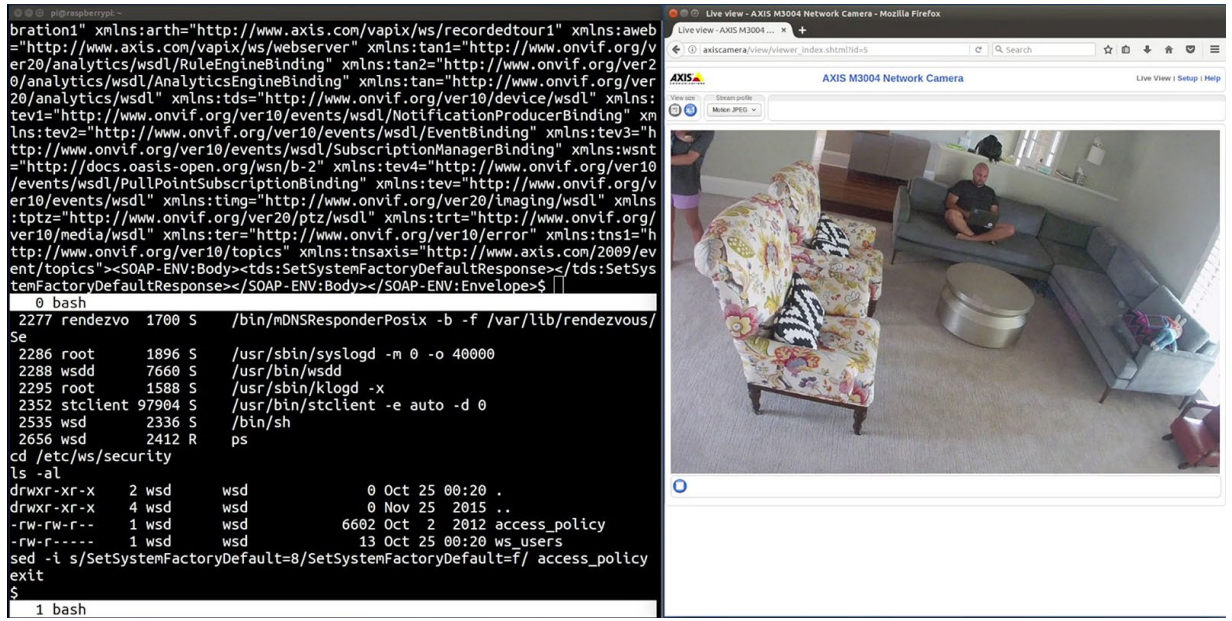
- Ripple20 Zero-Day Vulnerabilities in Treck TCP/IP Libraries
  - Popular IPv6 protocol implementation for embedded systems
  - Affected millions of devices in various industry sectors
- CVE-2020-11896
  - DNS Remote Code Execution vulnerability
- CVE-2020-11897, CVE-2020-11901
  - Inject shellcode on the device via ICMP tunneling
- Github lists 13 repositories related to Ripple20



RUBE-GOLDBERG ATTACK

- Exploits a vulnerability known as “Devil’s Ivy”
- CVE-2017-9765
- Affects over 250 camera models (mostly from AXIS)
  - Start by performing a Shodan search for AXIS
- The attacker can:
  - Factory reset the camera
  - Gain root access
  - Take over the device

https://vimeo.com/225922694

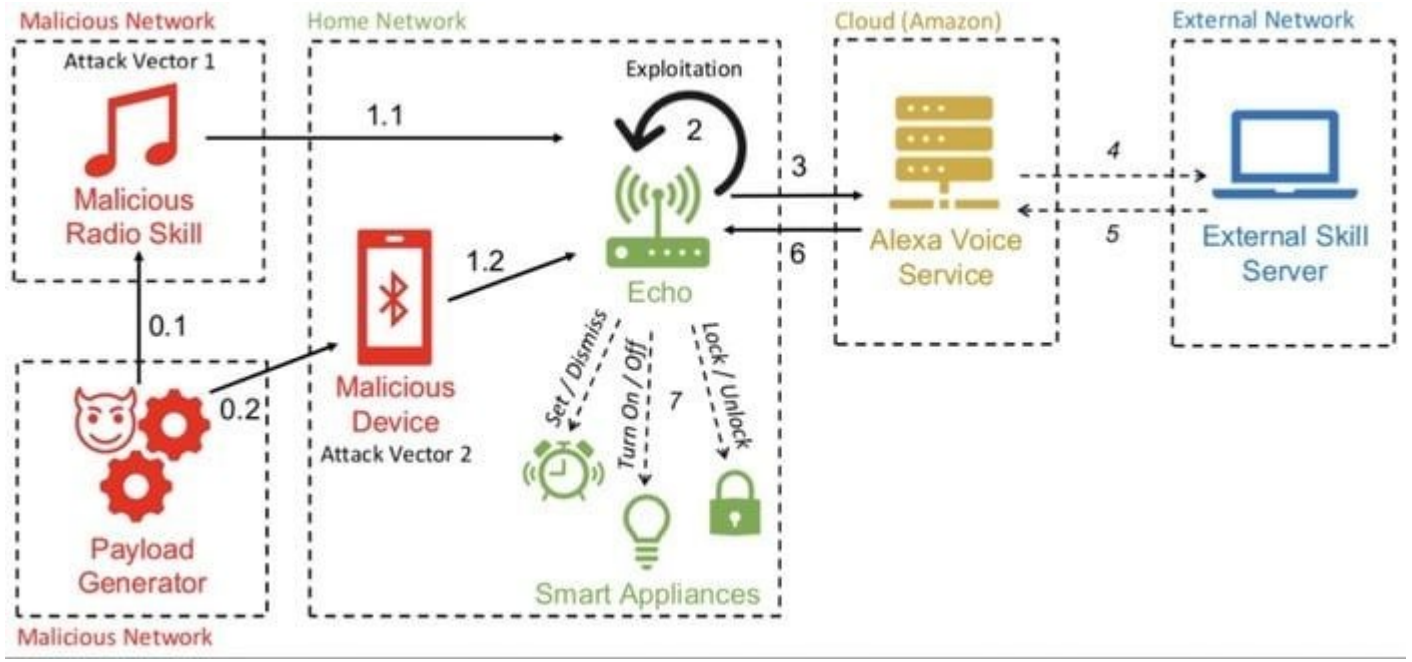


CLOUDPETS ATTACK

- Cloud-connecting children's toys can be turned into remote surveillance devices
- In 2017, an open MongDB database was found with personal information, hashed passwords and voice recordings of messages by children and parents using CloudPets teddy toys
- Exploit: https://github.com/pdjstone/cloudpets-web-bluetooth
- GitHub lists 10 more repos for CloudPets

AMAZON ECHO

- "Alexa vs Alexa" Full Volume Attack
- Attacker commands Echo to say malicious instruction commands to itself
- GitHub lists 3 repos with exploits for Alexis



TRENDNET WEBCAM

Multiple vulnerabilities:

- Remote Security Bypass
  - Search Shodan for TrendNet webcams
  - Append a string to the IP to access a hidden live stream
  - Example: http://<target IP>/anony/mjpg.cgi
- Multiple Buffer Overflows
  - Search exploit-db for “trendnet”

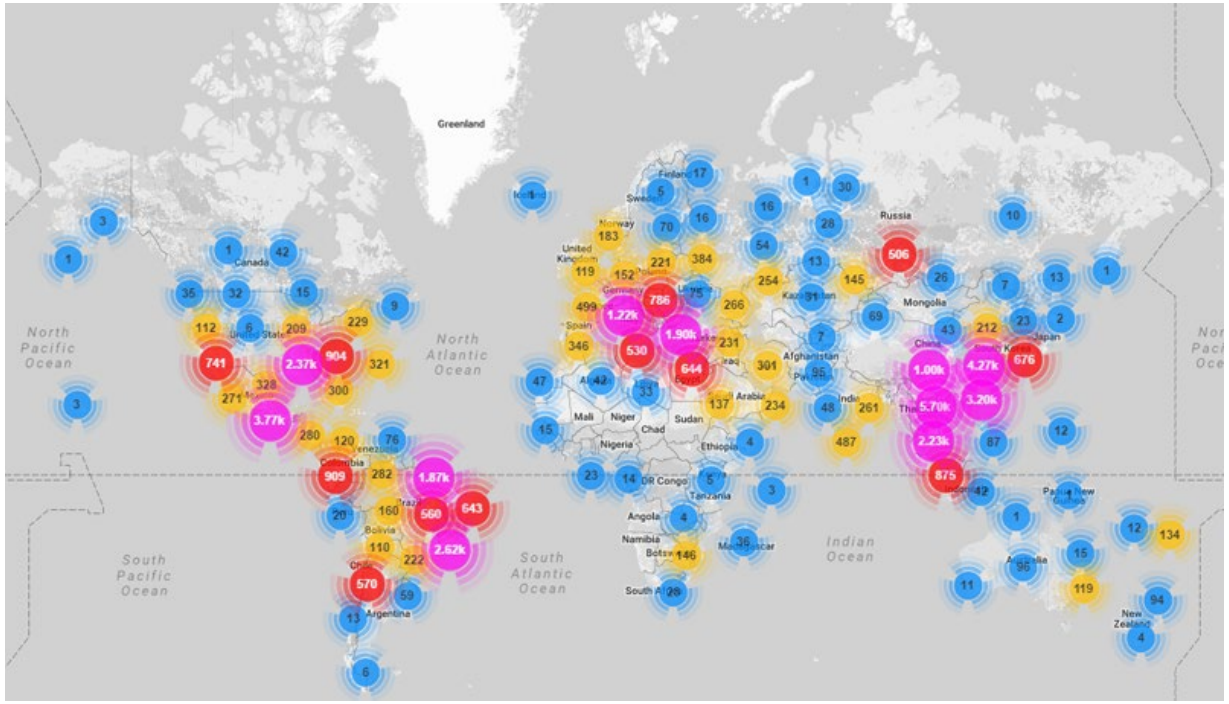
TESLA TBONE

- Zero-click exploit for Tesla Model 3 Media Control Unit (MCU)
  - Exploits two vulnerabilities affecting ConnMan
    - Internet connection manager for embedded devices
  - Remote code execution over Wi-Fi
- The Tesla automatically connects to the "Tesla Service" Wi-Fi SSID
  - Attacker used a drone to hover over the vehicle
  - Drone was running a Wi-Fi hotspot named "Tesla Service"
  - The car automatically connected
  - Attacker logged in using publicly available credentials
  - Took over the infotainment system

https://kunnamon.io/tbone/tbone-v1.0-redacted.pdf

MIRAI BOTNET DDOS ATTACK

- Mirai first grew a large botnet
  - Performed large IP block scanning to find devices with easy to crack credentials:
    - Factory defaults
    - Susceptible to brute forcing
  - 50,000 infected devices (mostly CCTV cameras)
  - Infections in 164 countries
- Then launched DDoS attacks based on instructions received from a remote C&C



https://github.com/lestertang/mirai-botnet-source-code/

18.5 IOT HACKING COUNTERMEASURES

- Defense
- Security Tools

DEFEND AGAINST IOT HACKING

- Today there are no longer clearly defined network perimeters
- Attacks are just as likely to pivot off a trusted internal user (phishing, drive-by malware) than through external means alone
- Defense in depth is not enough for IoT
- You must create a fabric of defense based on zero-trust and automation
  - Every connection and endpoint is considered a threat
  - Analyze activities in real-time
  - Automatically lock threats as they materialize

Use IoT to protect IoT

DEFEND AGAINST IOT HACKING (CONT'D)

- Approach security as a unified, integrated, holistic system
- Create an asset inventory and map out all possible ingress and egress paths
- Determine if the IoT network has its own (inappropriate/rogue) Internet gateway
- Disable guest and demo accounts if enabled
- Implement any existing lockout feature
- Implement the strongest available authentication mechanism
  - Prefer two-way authentication with SHA and HMAC hashing

DEFEND AGAINST IOT HACKING (CONT'D)

- Locate control system networks and devices behind firewalls
  - Isolate them from the business network
- Implement IDS/IPS on the network
- Implement end-to-end encryption using PKI when possible
- Use VPNs when possible
- Only allow trusted IP addresses to access the device from the Internet
- Disable UPnP ports on routers

DEFEND AGAINST IOT HACKING (CONT'D)

- Protect devices from physical tampering
- Patch vulnerabilities and update firmware if available
- Implement secure boot with cryptographic code signing when possible
- Monitor traffic on port 48101 as infected devices tend to use this port
- Ensure that a vehicle has only one identity
- Implement data privacy and protection as much as possible
- Implement data authentication, authenticity, and encryption wherever possible
- Use a CAPTCHA with account lockout to avoid brute forcing

DEFEND AGAINST IOT HACKING (CONT'D)

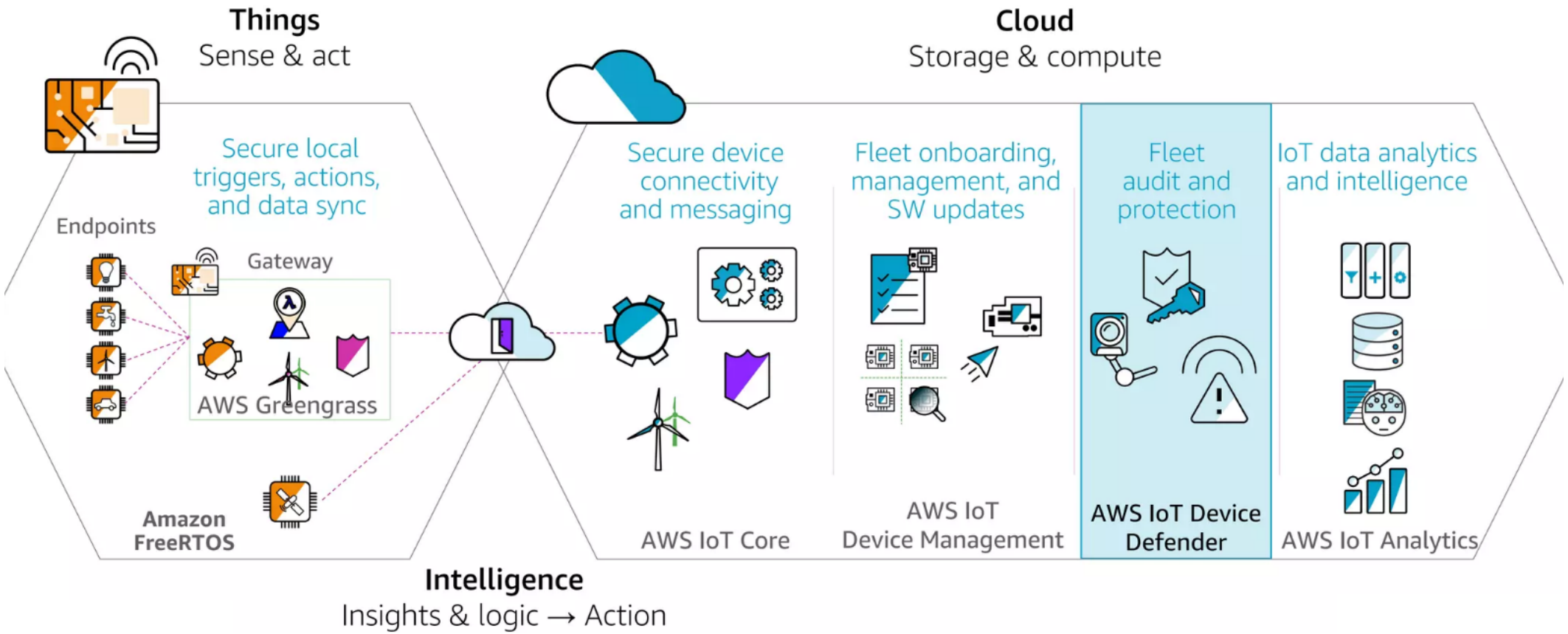
- Use a trusted execution environment (TEE) to secure sensitive information
- Validate code immediately before its use to reduce the risk of time-of-check to time-of-use (TOCTOU) attacks
- Secure encryption keys in a Secure Access Module (SAM), Trusted Platform Module (TPM) or Hardware Security Module (HSM)
- Disable WebRTC in the browser to prevent disclosure of IP addresses
- Use ad blockers and non-trackable browser extensions to prevent web-based attacks on IoT devices
- Consider using a SaaS platform Azure IoT Central to simplify IoT setup

IOT SECURITY TOOLS

- SeaCat.io
- DigiCert IoT Security Solution
- Pulse: IoT Security Platform
- Symantec IoT Security
- Google Cloud IoT
- Net-Shield
- Trustwave Endpoint Protection Suite
- NSFOCUS ADS

- Darktrace
- Noddos
- Cisco IoT Threat Defense
- AWS IoT Device Defender
- Zvelo0 IoT Security Solution
- Cisco Umbrella
- Carwall
- Bayshore Industrial Cyber Protection Platform

AWS IOT DEVICE DEFENDER EXAMPLE



18.6 OT CONCEPTS

- Operational Technology
- OT Terminology
- OT Components

OPERATIONAL TECHNOLOGY (OT)

- IoT focused on industry operations
- Used to monitor, run and control industrial process assets

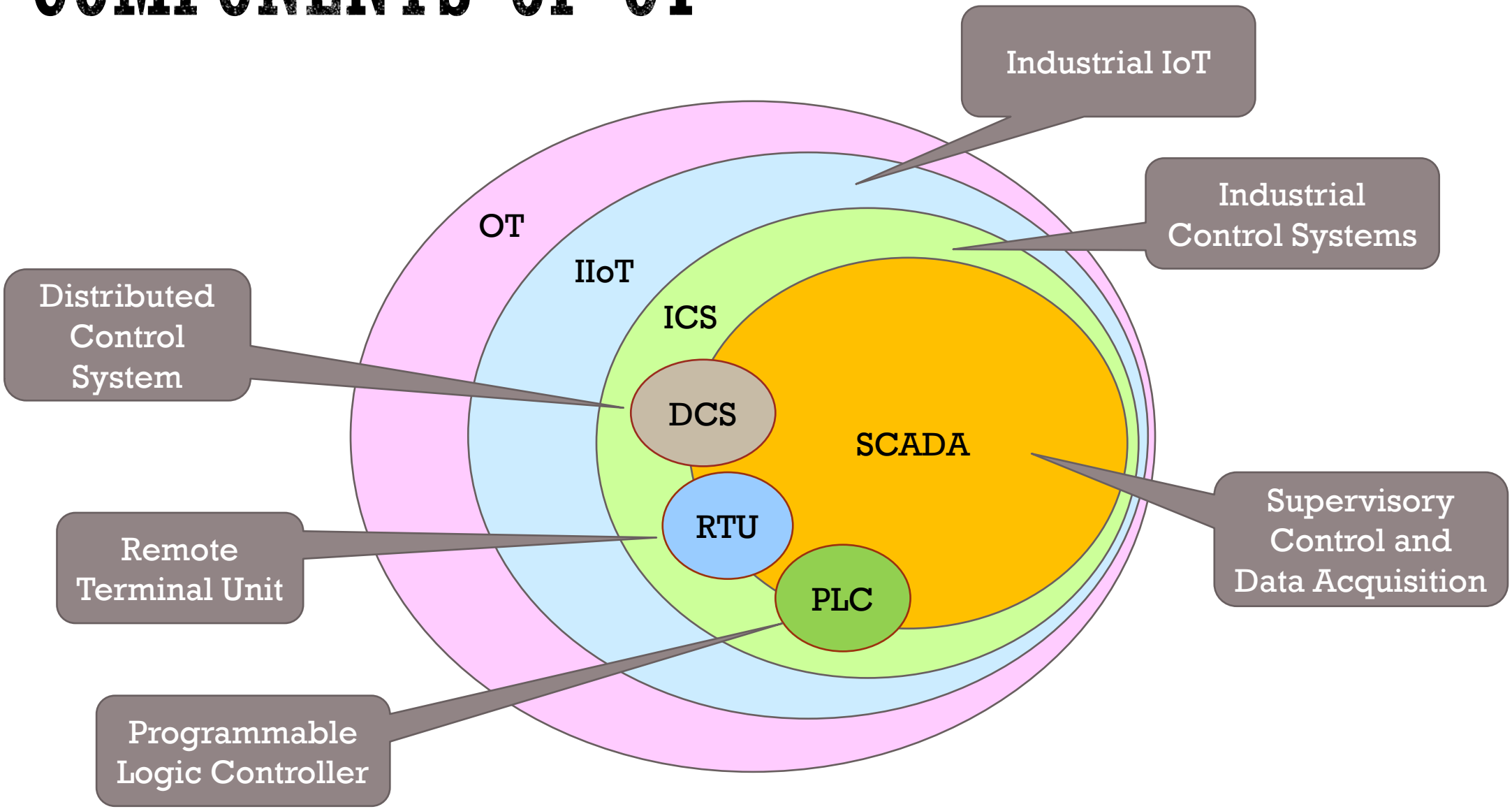
ESSENTIAL OT TERMINOLOGY

- Assets
  - Physical devices such as sensors, actuators, servers, workstations, network devices, programmable logic controllers (PLCs)
  - Logical assets such as flow graphics, program logic, databases, firmware, firewall rules
- Zones and Conduits
  - A network segregation technique
  - Isolates networks and assets into security zones to impose strong access control
- Industrial Network
  - A network of automated control systems
- Business Network
  - AKA Enterprise network
  - A "normal" IT network of systems that provide information infrastructure for the business

ESSENTIAL OT TERMINOLOGY

- Industrial Protocols
  - Protocols such as (proprietary) S7, CDA, SRTP and (non-proprietary) Modbus, OPC, DNP3, CIP
  - Used for serial communication or over standard Ethernet
- Network Perimeter
  - Outermost boundary of a network zone
- Electronic Security Perimeter
  - Boundary between secure and insecure zones
- Critical Infrastructure
  - A collection of physical or logical systems and assets
  - If it fails or is destroyed it would severely impact security, safety, the economy, or public health

COMPONENTS OF OT



INDUSTRIAL IOT

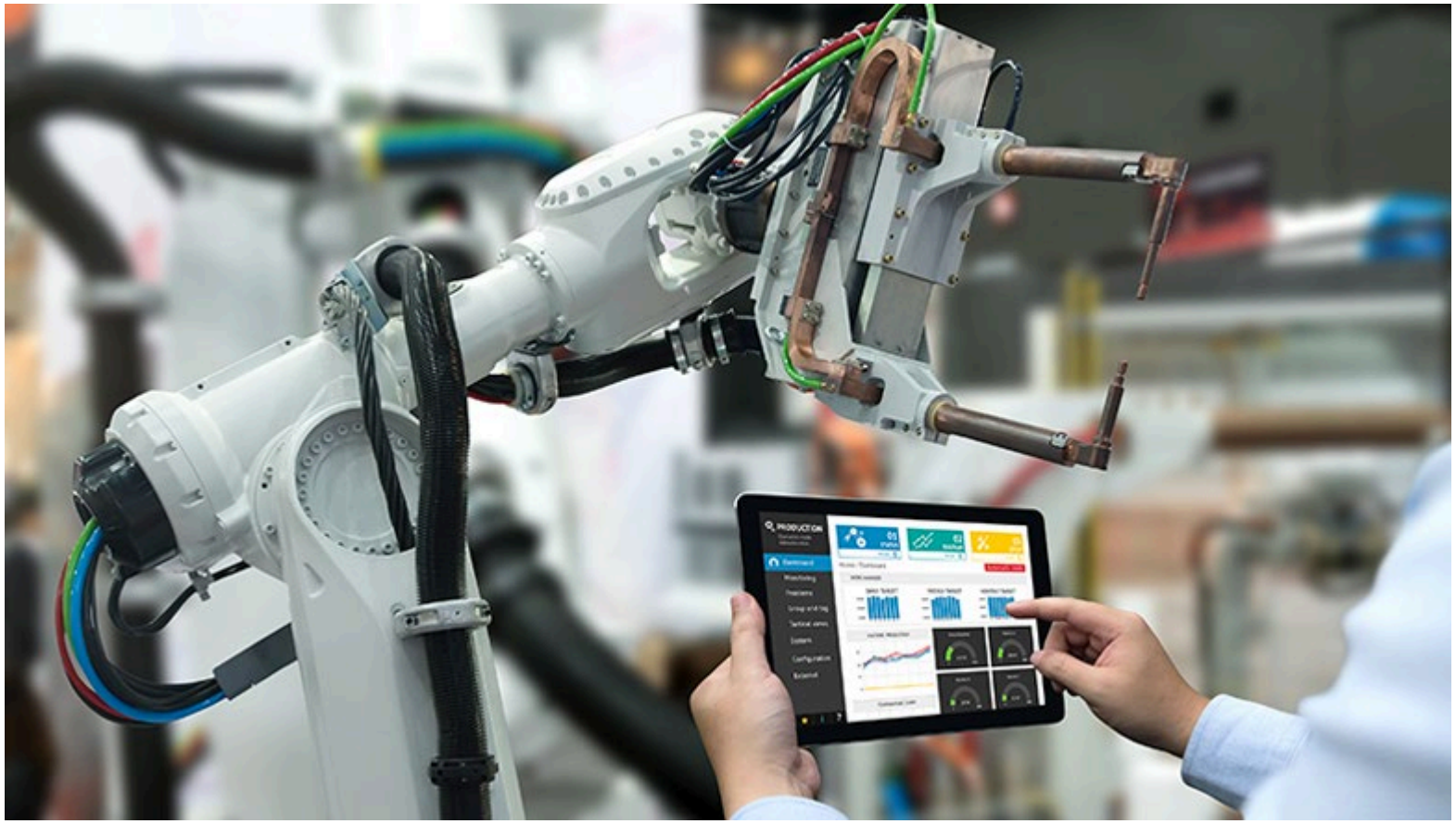
- IIoT

INDUSTRIAL IOT (IIOT)

- A subset of the larger IoT
- The use of IoT in industrial sectors and applications
  - Including robotics, medical devices, and software-defined production processes
- Collect and share data between devices to make decisions without human interaction
- Strong focus on:
  - Machine-to-machine (M2M) communication
  - Big Data
  - Machine learning
- Leverages cloud-based serverless architecture for large scale analytics
  - Data from individual SCADA systems feed IIOT
- IIoT enables industries and enterprises to have better efficiency and reliability in their operations

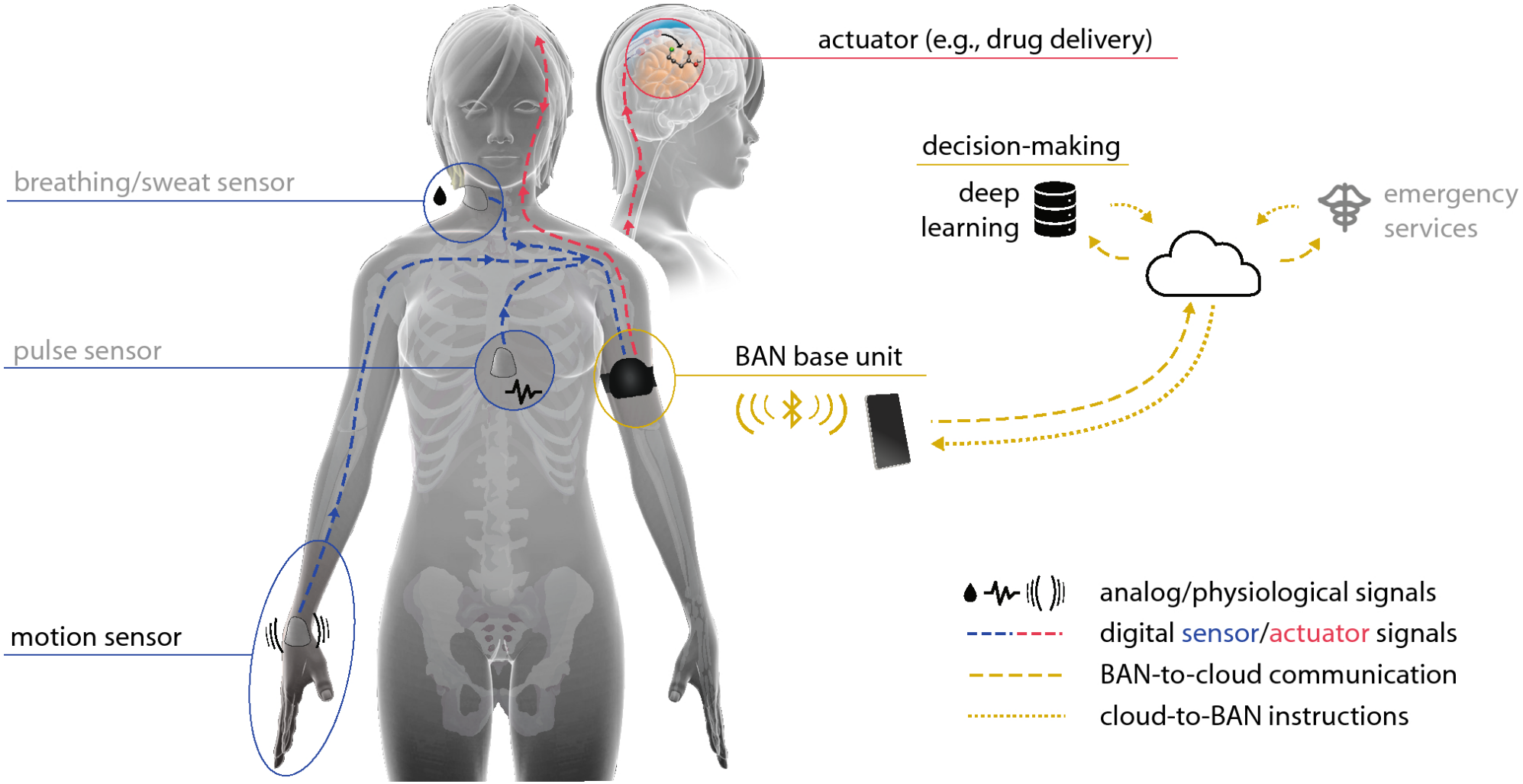
EVOLUTION OF INDUSTRY TO IIOT

IIOT MANUFACTURING EXAMPLE



IIOT RETAIL EXAMPLE

IIOT HEALTHCARE EXAMPLE



IIOT AGRICULTURE EXAMPLE

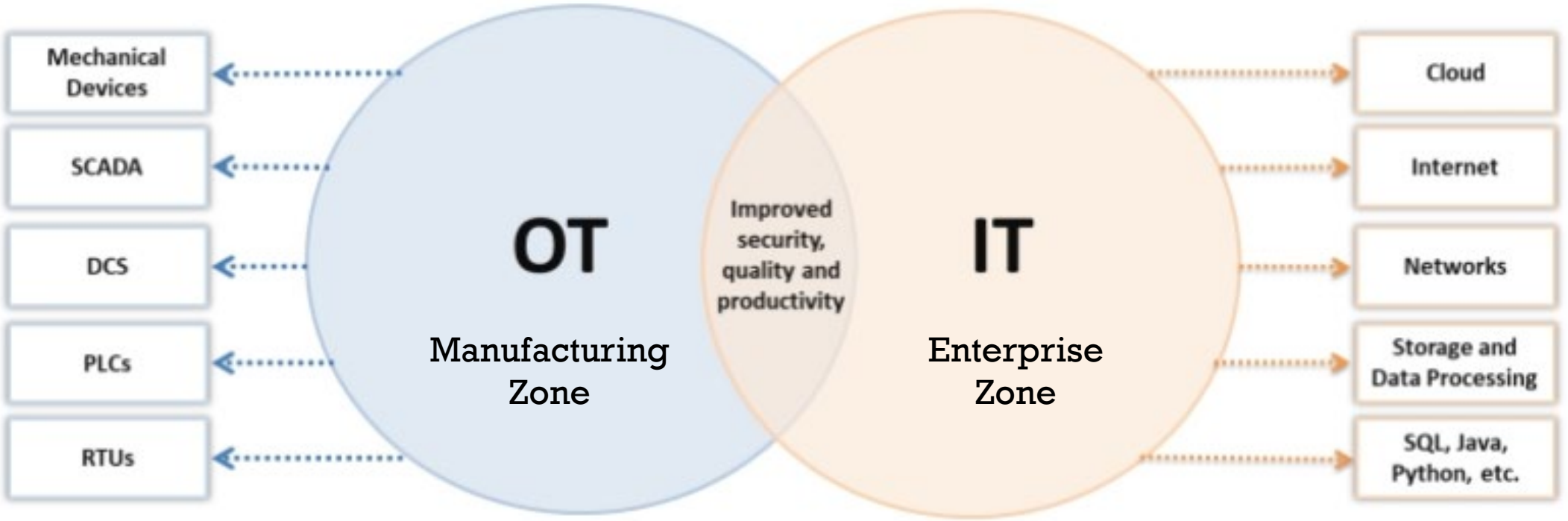
IIOT AGRICULTURE EXAMPLE #2

18.7 IT-OT CONVERGENCE

- IT and OT
- Enterprise Zone
- Manufacturing Zone
- Protecting the OT Network

IT-OT CONVERGENCE

- These two work together
- Keep the two networks separate!



ENTERPRISE ZONE

- IT Systems
  - Technologies and protocols:
    - DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4, IPv6, OPC, TCP/IP, Wi-Fi
- Level 5 - Enterprise Network
  - Business-to-Business (B2B)
  - Business-to-Customer (B2C)
  - Accumulates data from subsystems at individual plants
  - Aggregates inventory and overall production status
- Level 4 - Business Logistics Systems
  - IT systems that support production
  - Application, file, and database servers
  - Supervising systems
  - Email systems

MANUFACTURING ZONE

- OT Systems
- Level 3 - Operational Systems/Site Operations
  - Technologies and Protocols:
    - CC-Link, DDE, G-SRTP, HSCP, ICCP, MODBUS, NTP, Profinet, SuiteLink, Tase-2, TCP/IP
- Level 2 - Control Systems/Area Supervisory Controls
  - Technologies and Protocols:
    - 6LoWPAN, CC-Link, DNP3, DNS/DNSSEC, FT, HART-IP, IEC 60870-5-101, IPv4/IPv6, ISA, OPC, NTP, SOAP, TCP/IP
- Level 1 - Basic Controls/Intelligent Devices
  - Technologies and Protocols:
    - BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 624423, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7, WiMax

PROTECTING OT FROM IT

- Enterprise and manufacturing zones are often connected via Ethernet
- A standalone, unconnected ("islanded") OT system is inherently safer from outside threats than one connected to an enterprise IT system(s)
  - Nearly all enterprise networks have external connectivity
- An intermittently connected OT system can be a good compromise
  - It is only at risk when it is connected
  - Connections should be on a need-basis such as for downloading updates or limited-time remote access
- The most common external connectivity into the OT environment is 3rd party connections from vendors
  - Their risk becomes your risk

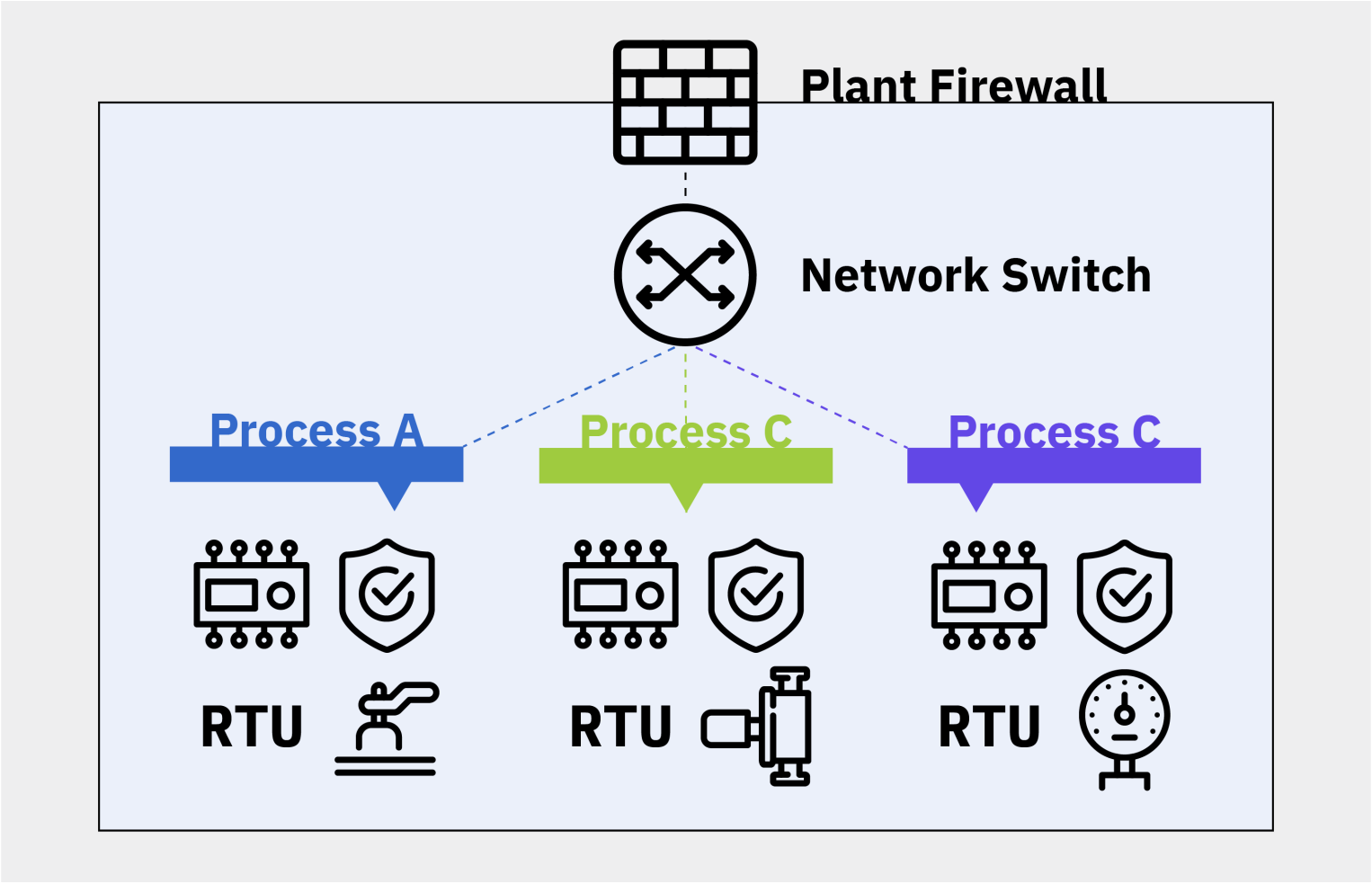
18.8 OT COMPONENTS

- ICS
- SCADA
- PLC
- HMI
- RTU
- DCS
- Additional OT Components
- The Complete Picture

INDUSTRIAL CONTROL SYSTEMS (ICS)

- Collection of different types of control systems such as:
  - SCADA, DCS, BPCS, SIS, HMI, PLCs, RTU, IED
- ICS is extensively used in:
  - electricity production and distribution
  - water supply and waste-water treatment
  - oil and natural gas supply
  - chemical and pharmaceutical production
  - pulp and paper
  - food and beverages

ICS EXAMPLE


Plant Firewall
Network Switch
Process A
Process C
Process C
RTU
RTU
RTU

ICS CONFIGURATION

- ICS systems are configured in one of three modes:
  - Open loop
    - Output of the system depends on the preconfigured settings
  - Closed loop
    - The output always has an effect on the input to acquire the desired objective
  - Manual mode
    - The system is totally under the control of humans

SCADA

- SCADA Overview

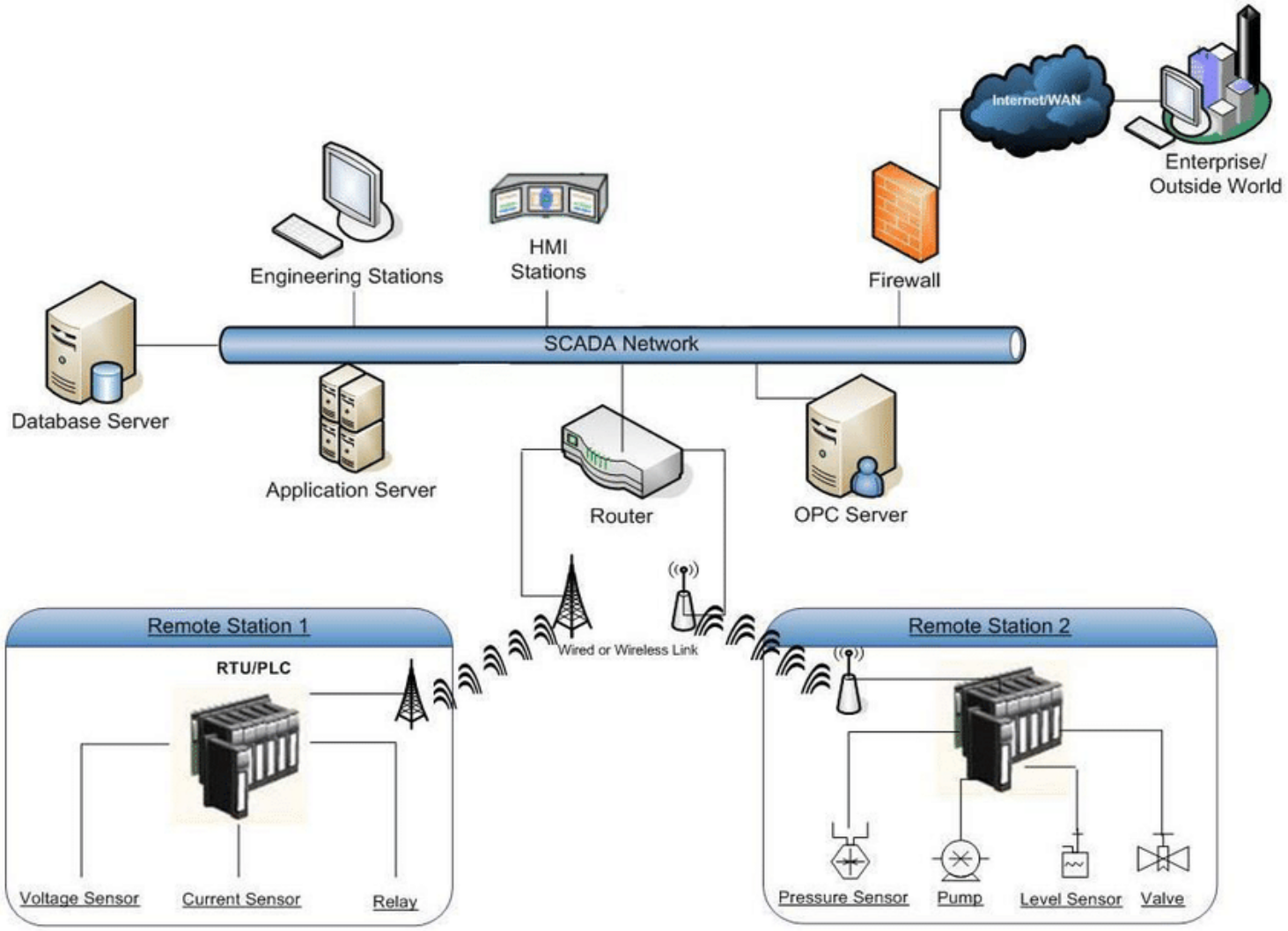
SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

- A subset of ICS
- A centralized supervisory control system
  - Provides central supervision over a variety of proprietary systems
- Used for controlling and monitoring:
  - Industrial facilities and infrastructure
  - Multiple process inputs and outputs

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) (CONT'D)

- Integrates data acquisition with data transmission and Human Machine Interface (HMI) software
  - HMI - Touch-screen operator control
  - RTU (Remote Terminal Unit) - Suitable for wider geographical telemetry; transmits telemetry data from field instruments directly to master control systems
  - PLC (Programmable Logic Controller) - Can autonomously, locally, execute simple logic processes without involving the supervisory computer
- In the past, depended on "security through obscurity"
- Now largely uses web technologies for human-system interaction

SCADA ARCHITECTURE EXAMPLE



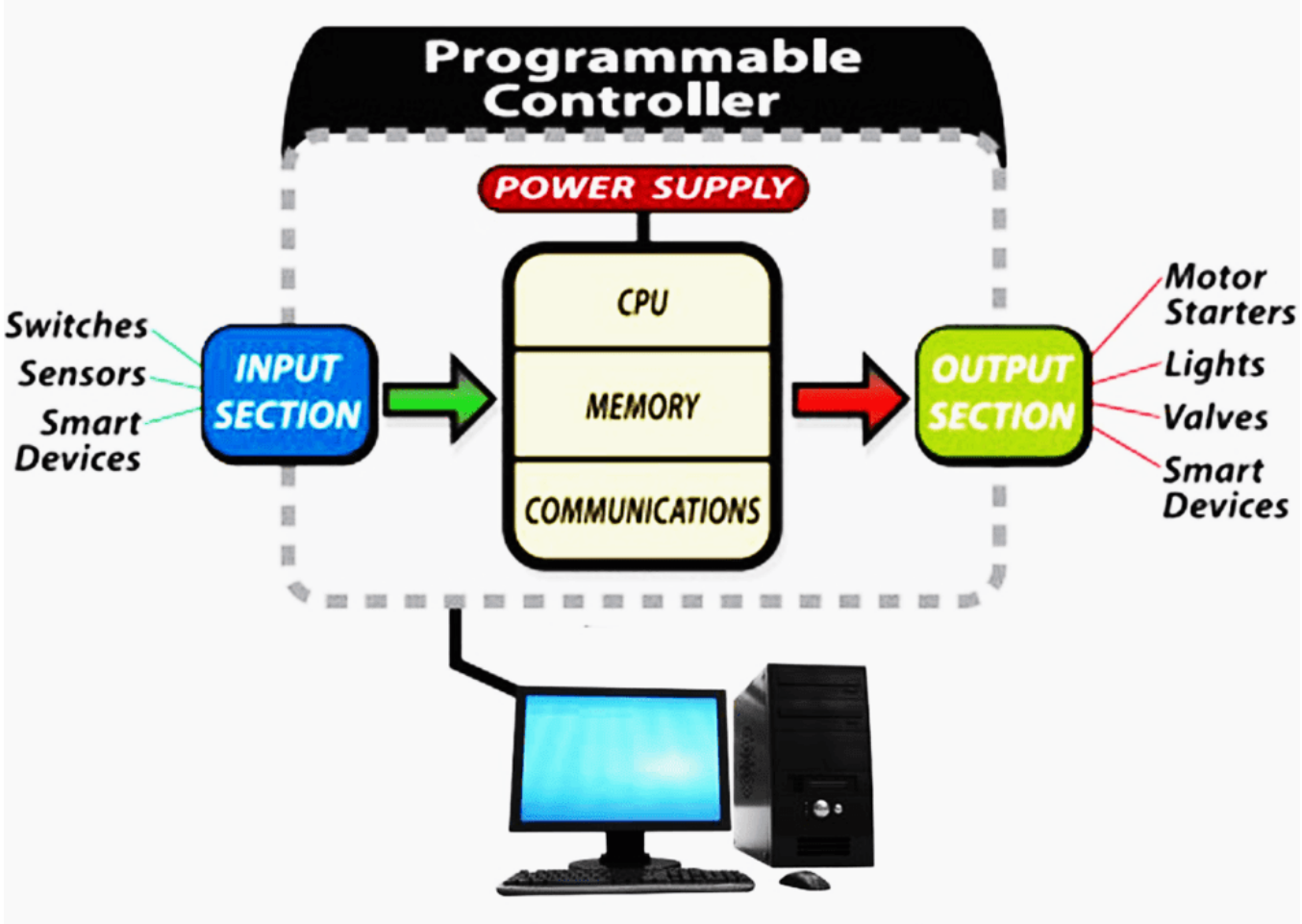
PLC

- Programmable Logic Controller

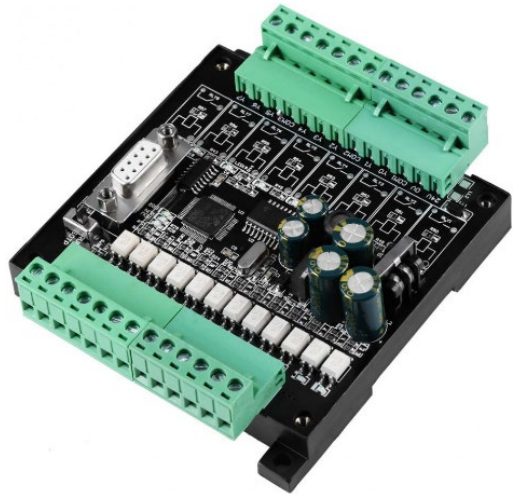
PROGRAMMABLE LOGIC CONTROLLER

- A small, solid-state control computer
- Controls a local process autonomously
- You can customize its instructions to perform a specific task
- Has a CPU module, and power supply module, and I/O modules
- Connects to other components via:
  - RS-232 serial cables
  - Modbus RTU serial cables
  - Ethernet TCP/IP
  - Modbus TCP/IP
  - Profinet

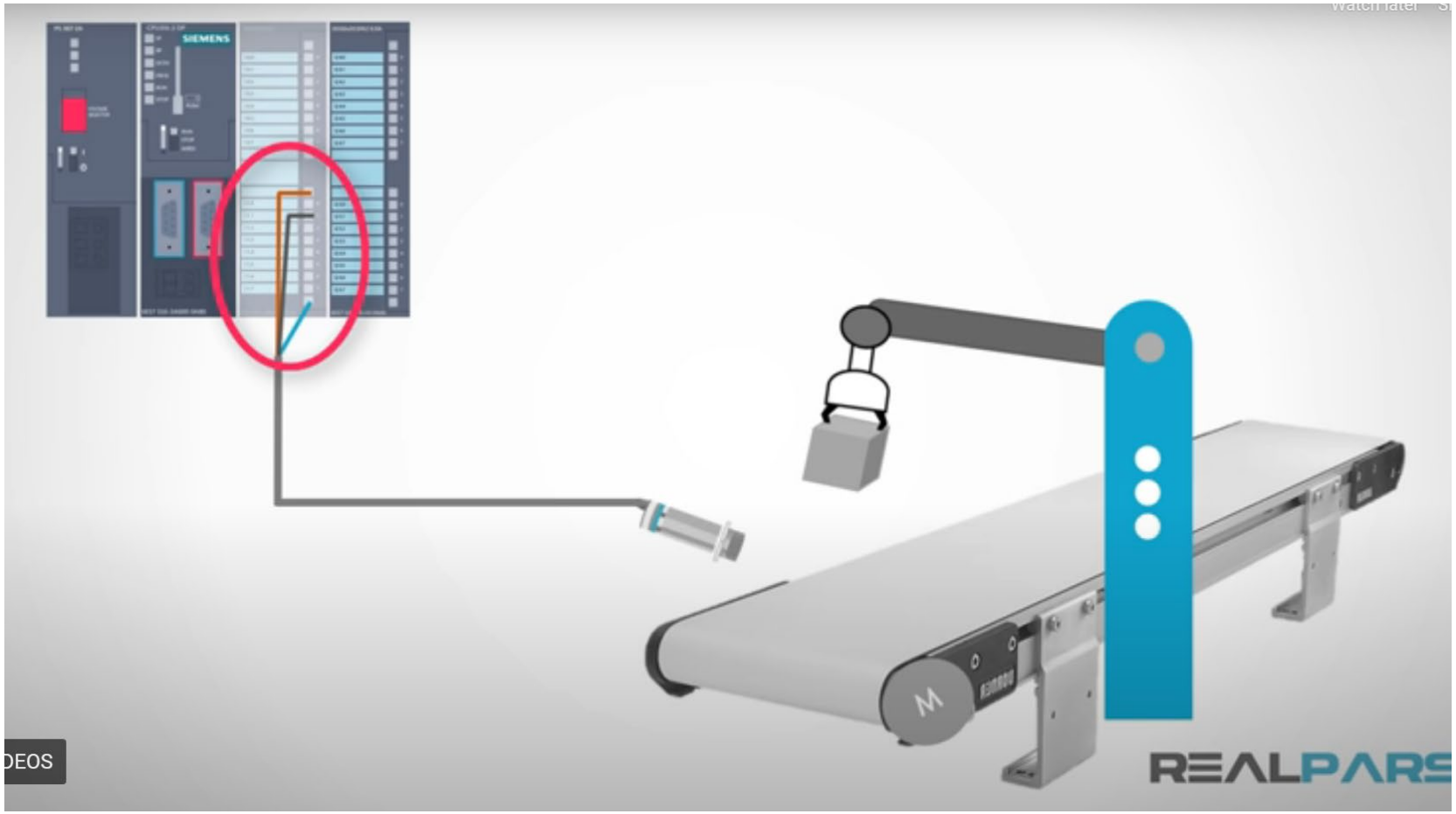
PLC ARCHITECTURE



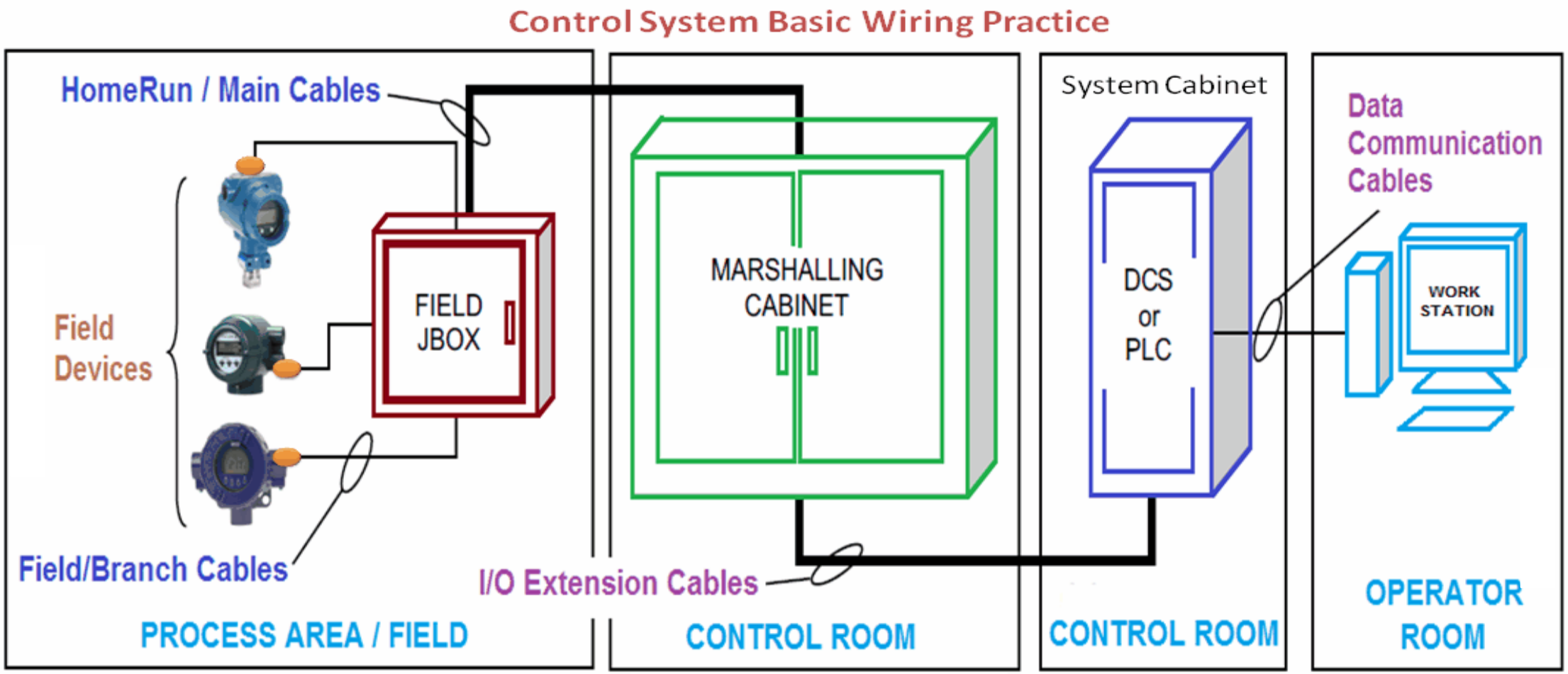
PLC EXAMPLES



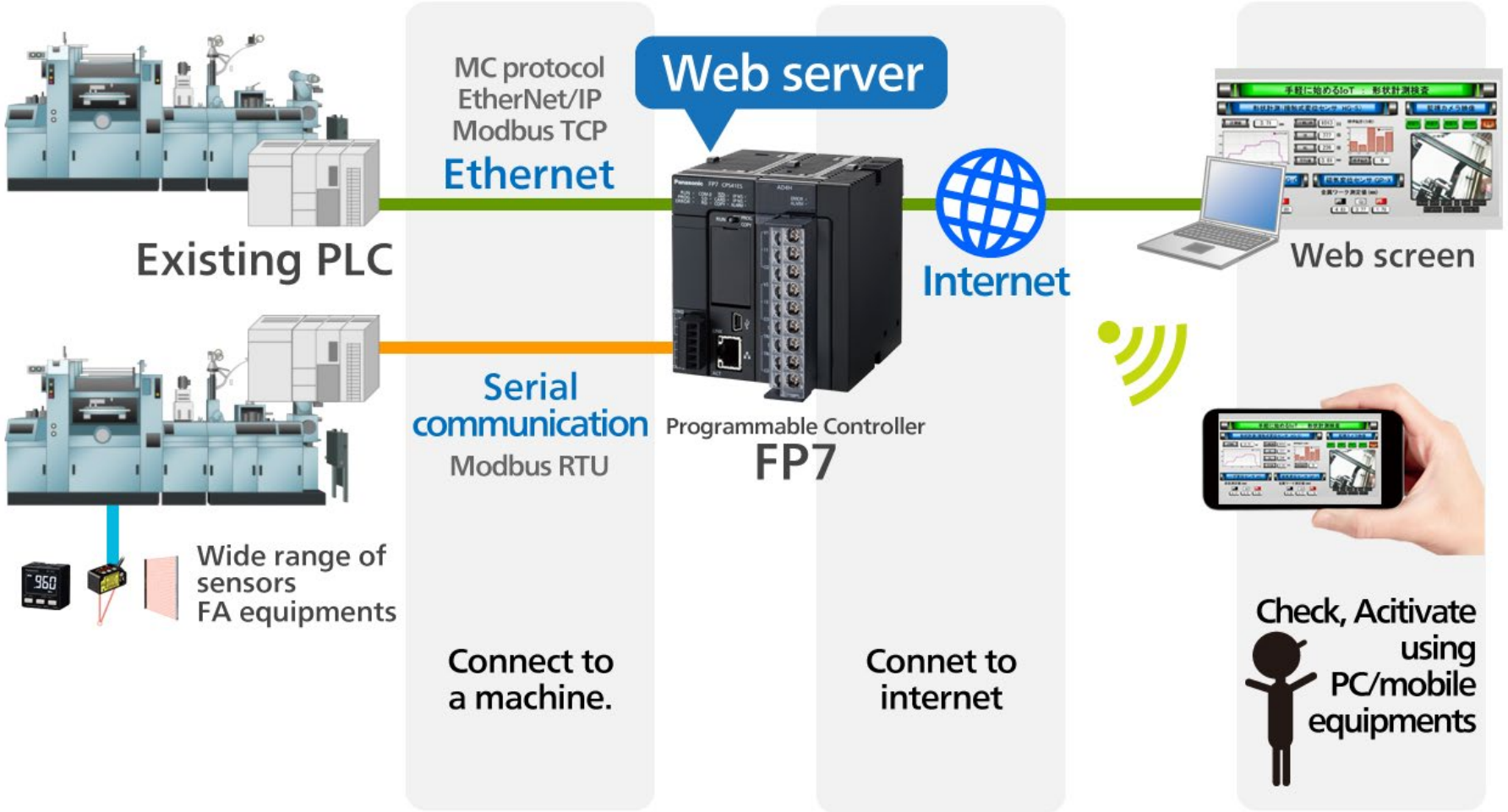
SENSOR WIRED TO A PLC EXAMPLE



TYPICAL PLC WIRING



REMOTE PLC EXAMPLE



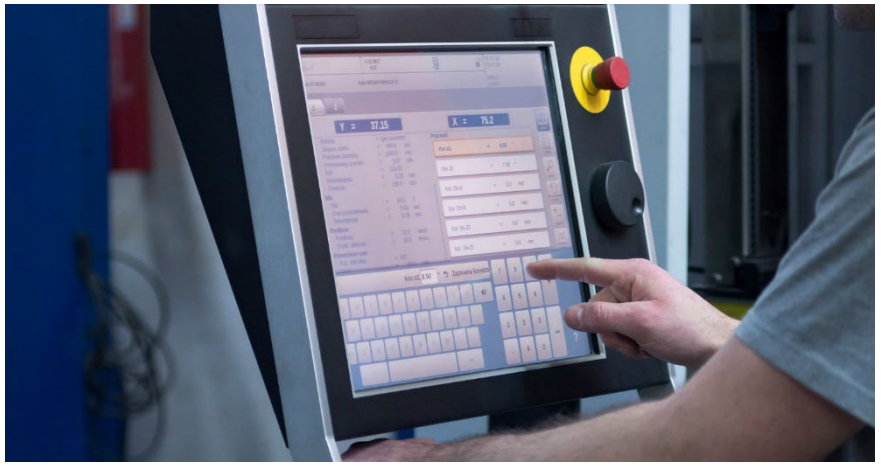
HMI

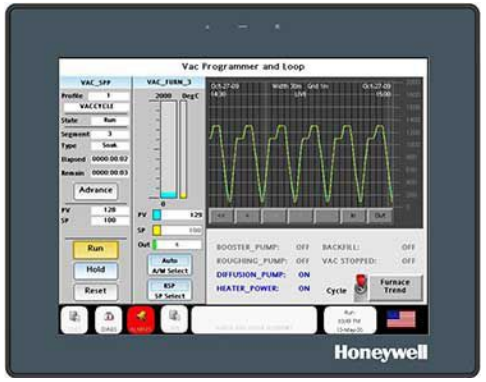
- Human-Machine Interface

WHAT IS AN HMI?

- Any interface or dashboard that connects a person to a machine
- Typically a touch screen used in an industrial process
- HMIs communicate with Programmable Logic Controllers (PLCs) and input/output sensors
- They get and display information for users to view
- They can send commands
- HMI screens can be used for:
  - A single function like monitoring and tracking
  - Performing more sophisticated operations like switching machines off or increasing production speed

HMI EXAMPLES





RTU

- Remote Terminal Unit

REMOTE TERMINAL UNIT (RTU)

- AKA Remote Telemetry Unit or Remote Telecontrol Unit
- Microprocessor-based device
- Typically installed in a remote location as part of a large system
- Monitors and controls field devices
  - valves, actuators, sensors, and more
- Connects to a distributed control system or SCADA
- Transmits telemetry data to a master system
- Uses messages from the master supervisory system to control connected objects

RTU EXAMPLES

PLC VS RTU

- Similar but not the same
- PLCs and RTUs have some overlapping functionality

PLC	RTU
• Used for output control of devices like valves, pumps, motors, etc.	• Generally not used for output control
• Wired connectivity	• Wireless connectivity
• Local use	• Wider geographical telemetry
• Might have built-in display • Connection to SCADA not a requirement	• No built-in display • Must be connected to SCADA
• Cheaper	• More expensive

DCS

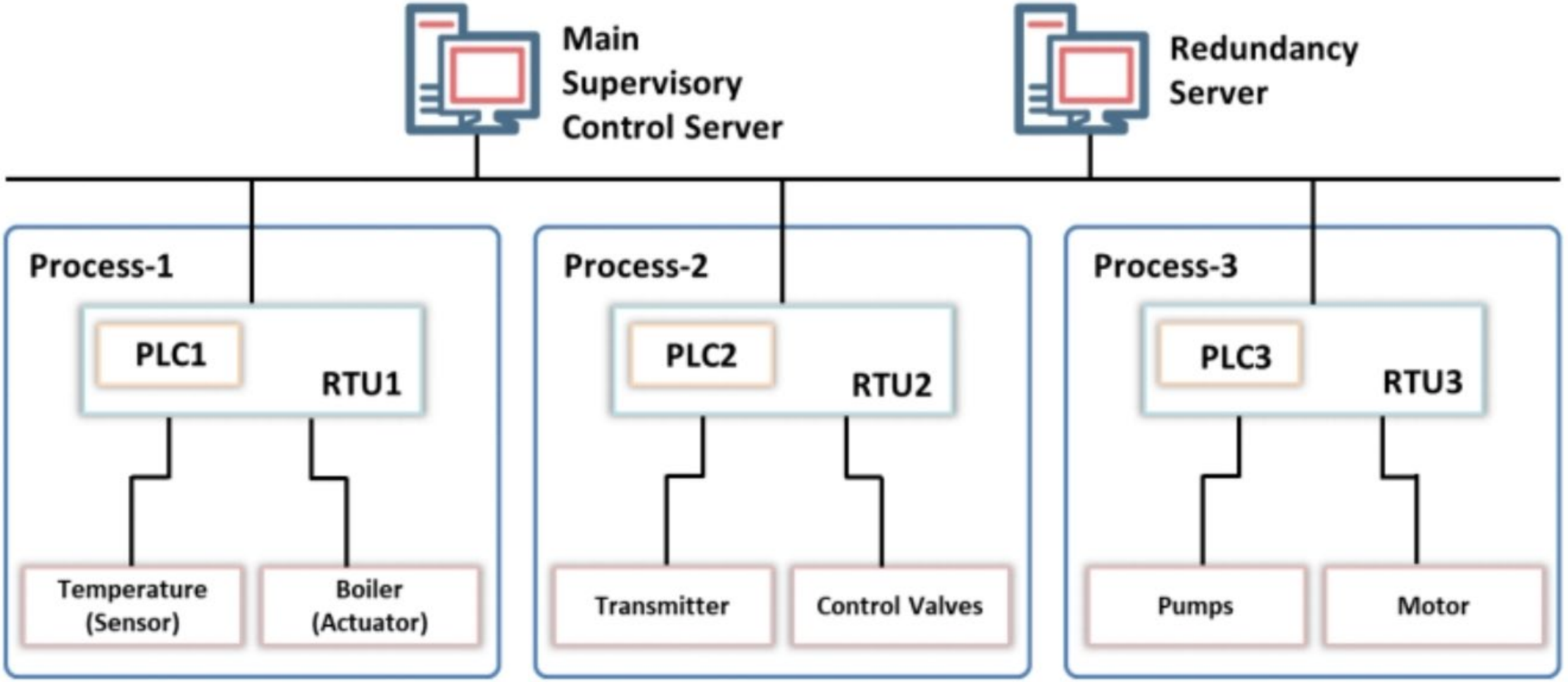
- Distributed Control System

DISTRIBUTED CONTROL SYSTEM

- A highly engineered large-scale control system
- Often used to perform industry-specific tasks
- Contains a centralized supervisory control unit
- Used to control:
  - Multiple local controllers
  - Thousands of I/O points
  - Various other field devices
- Operates using a centralized supervisory control loop (SCADA, MTU*)
  - Connects a group of localized controllers (RTU/PLC)
  - Executes the overall tasks required for the entire production process
  - Used to control production systems spread within the same geographical location
- For industry-specific tasks
- Large, complex, distributed processes such as:
  - Chemical manufacturing, nuclear plants, oil refineries, water and sewage treatment plants, electric power generation, automobile and pharmaceutical manufacturing

* Master Terminal Unit - the heart of the SCADA system

DISTRIBUTED CONTROL SYSTEM (DCS)



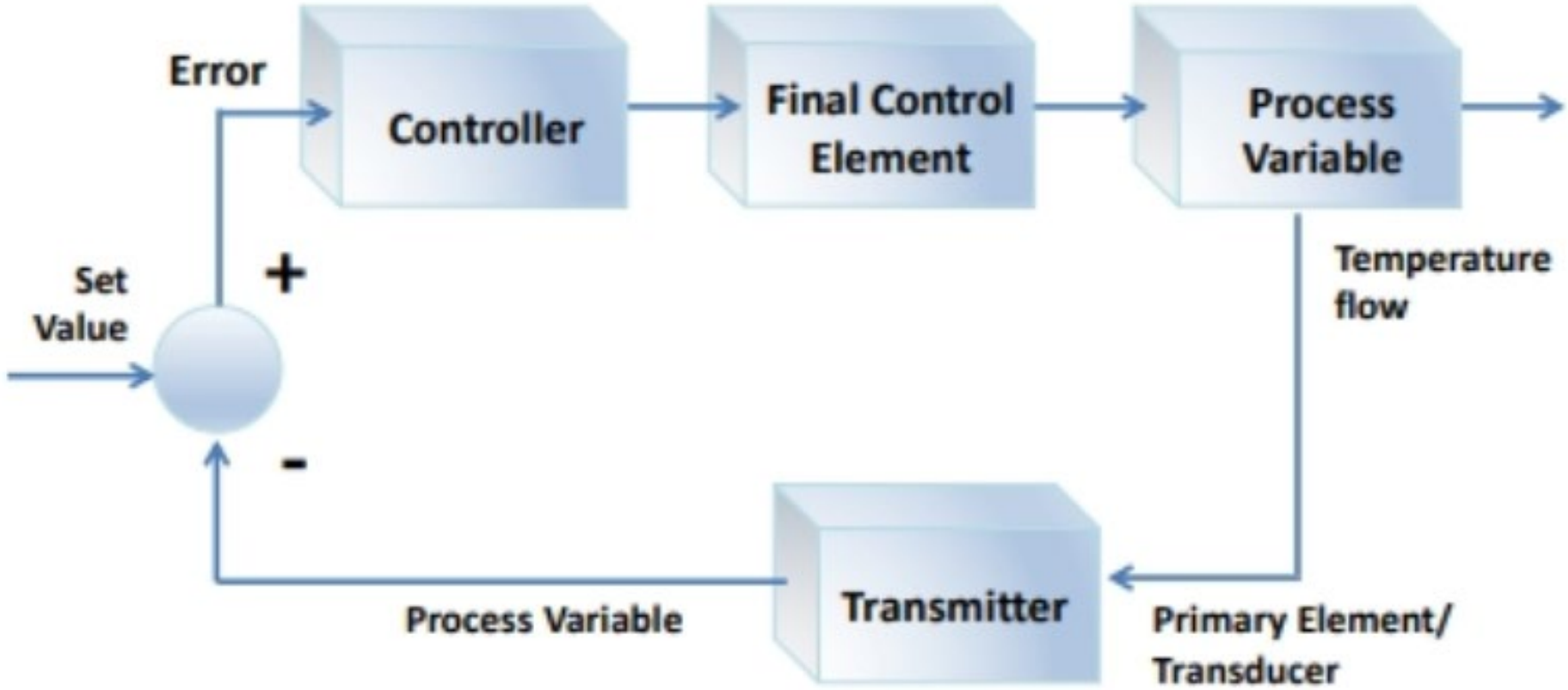
ADDITIONAL OT COMPONENTS

- BPCS
- SIS

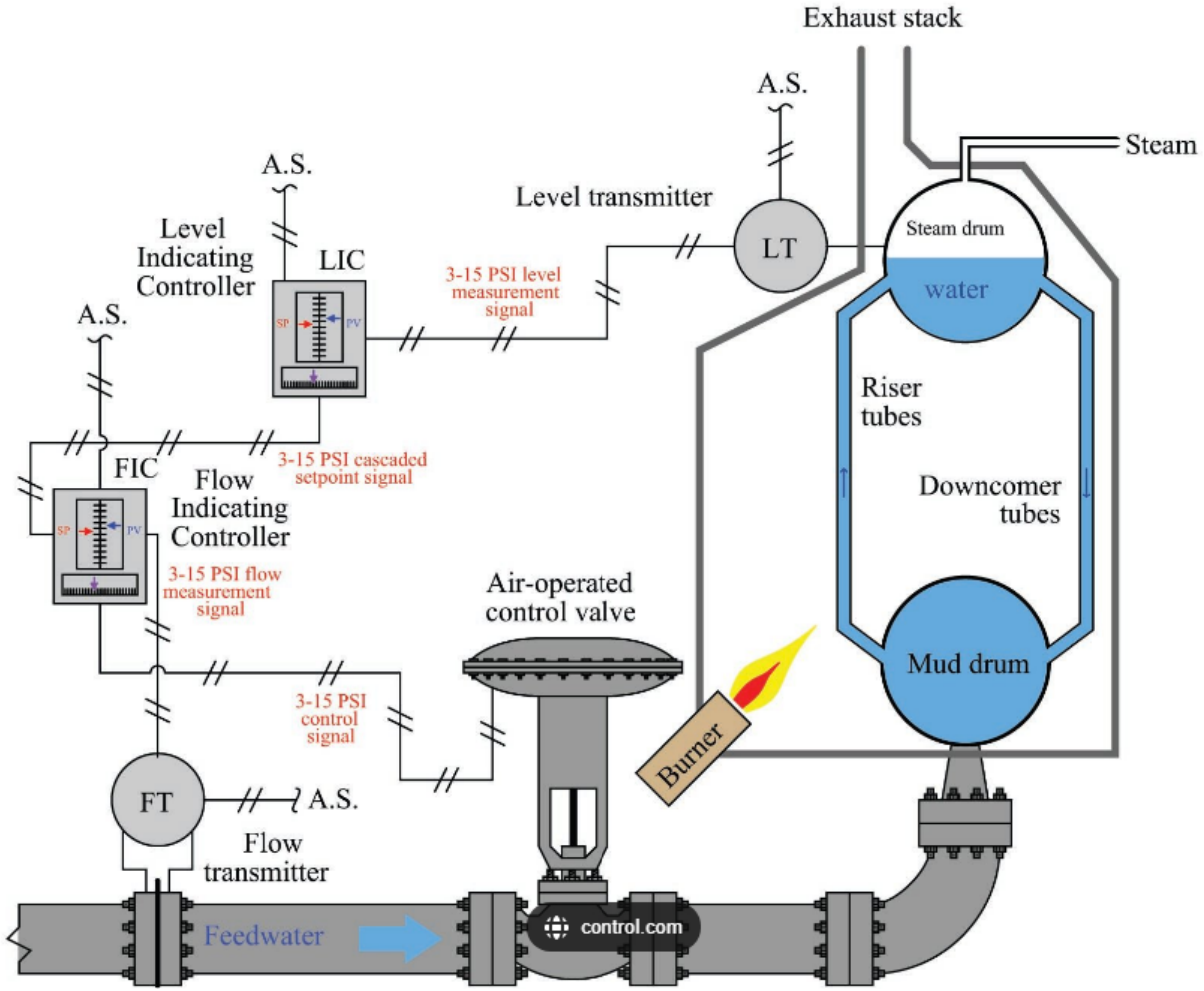
BASIC PROCESS CONTROL SYSTEM (BPCS)

- Responsible for process control and monitoring of the industrial infrastructure
- Responds to input signals from the process and associated equipment
- Generates output signals that make the process and equipment operate as required
- Commonly used in feedback loops such as:
  - Temperature control
  - Batch control
  - Pressure control
  - Flow control
  - Feedback and feed-forward controls for chemical, oil and gas, and food and beverage

BPCS CLOSED LOOP ARCHITECTURE



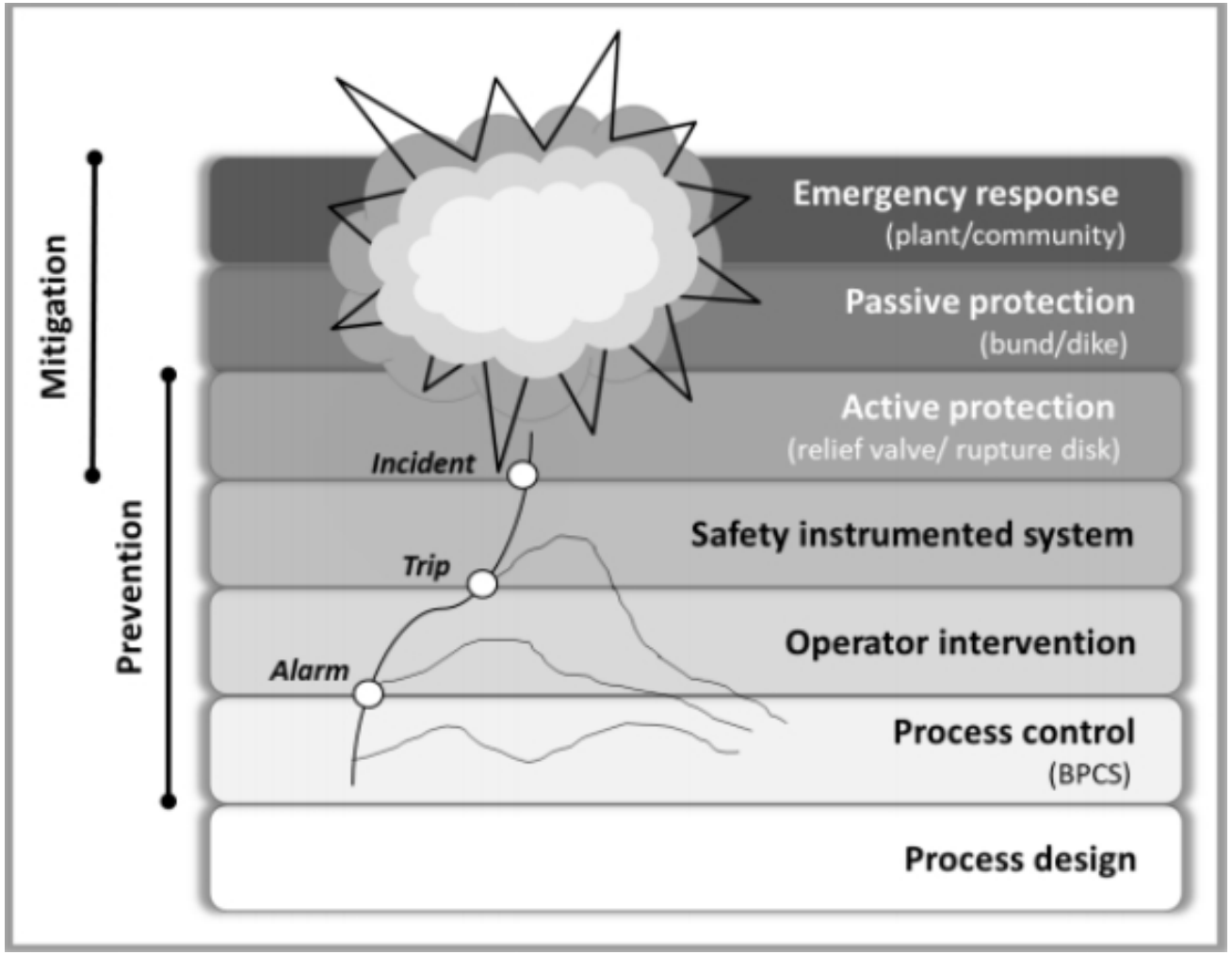
BCPS EXAMPLE - 2 ELEMENT BOILER STEAM DRUM



SAFETY INSTRUMENTED SYSTEM (SIS)

- Automated control system designed to safeguard the manufacturing environment
- Automatically shuts down the system in case of a hazardous incident
  - Overrides the BPCS
- Part of risk management strategy

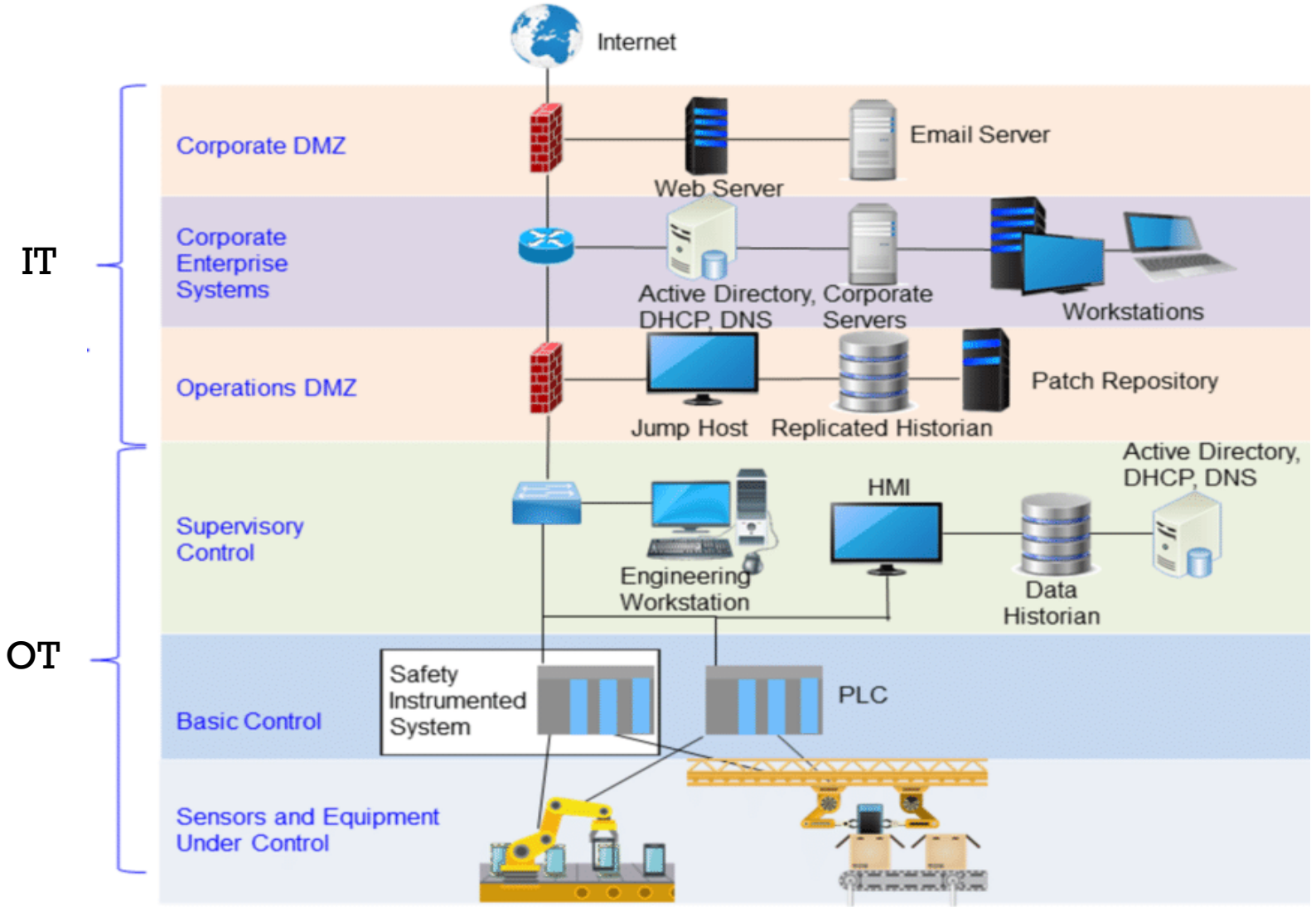
SIS LAYERS OF PROTECTION



THE COMPLETE PICTURE

- IT and OT Together

PUTTING IT ALL TOGETHER



18.9 OT VULNERABILITIES

- OT Challenges
- Common OT Vulnerabilities
- Well-Known Attacks

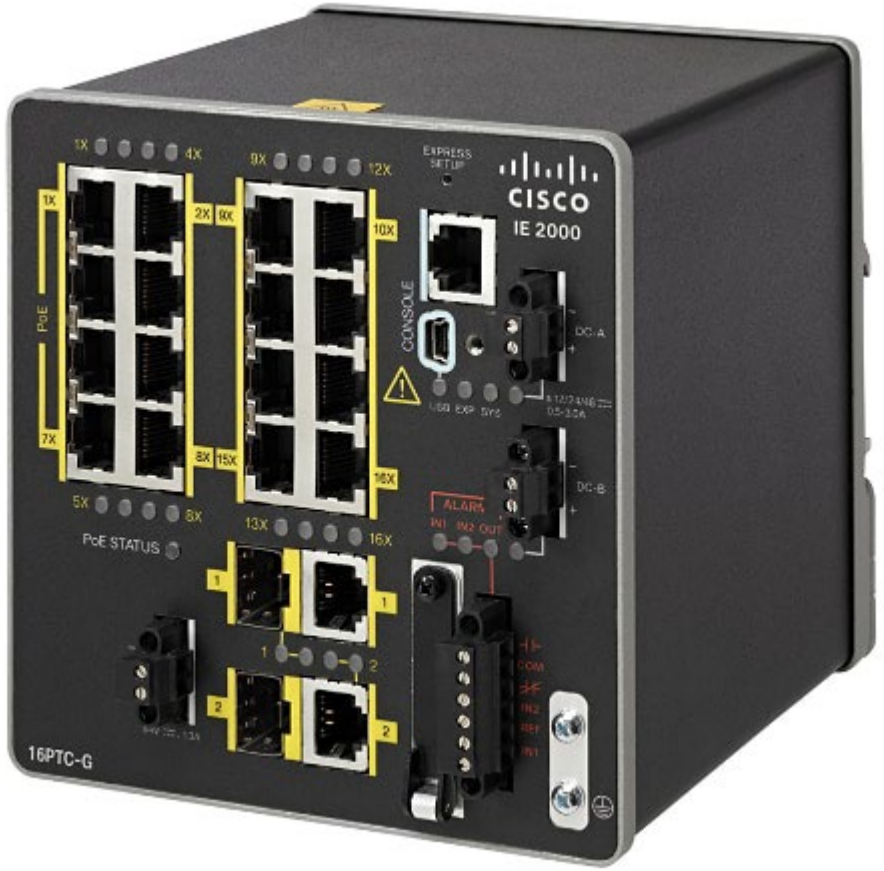
OT'S BIGGEST SECURITY CHALLENGE

- ICS and SCADA systems are difficult to retrofit with modern security
- Most were developed many years before security standards were established and integrated into their design
  - Many of these older systems date back to the 1970s and are still in use today
- Over time, these systems were incorporated into the organization's TCP/IP data networks
  - This provides a huge exploitation area by penetration testers and attackers alike

OT'S BIGGEST SECURITY CHALLENGE (CONT'D)

- Many ICS and SCADA vendors are slow to implement security measures
  - Because they cannot be easily retrofitted with the newer security requirements
- For example, some ICS/SCADA systems use a proprietary operating system
- More modern ICS/SCADA operates using a version of Windows
- However, many still use Windows XP, making them much more vulnerable since they cannot be upgraded to Windows 10 without hardware replacement
- ICS and SCADA systems should ALWAYS be isolated from production networks and segmented into their own logical networks (VLANs)

CISCO INDUSTRIAL SWITCH FOR ICS EXAMPLE



OT CHALLENGES

- Lack of visibility
- Plaintext/weak passwords
- Network complexity
- Legacy technology
- Lack of antivirus protection
- Lack of skilled security professionals
- Rapid pace of change
- Outdated systems

OT CHALLENGES (CONT'D)

- Haphazard modernization
- Insecure connections
- Usage of rogue devices
- Convergence with IT
- Organizational challenges
- Unique production networks/proprietary software
- Vulnerable communication protocols
- Remote management protocols

COMMON OT VULNERABILITIES

Vulnerability	Description
Publicly Accessible OT Systems	• OT systems that are directly connected to the Internet for the convenience of vendor maintenance • OT systems not protected by modern security controls • Ability to perform password brute-forcing or probe OT systems to disable or disrupt their functions
Insecure Remote Connections	• Corporate networks use jump boxes to establish remote connectivity to the ICS/SCADA network • Attackers exploit vulnerabilities in those jump boxes
Missing Security Updates	• Outdated software versions lead to increased risk and provide a path for attackers to compromise a system
Weak Passwords	• Use of default usernames and passwords for OT systems

COMMON OT VULNERABILITIES (CONT'D)

Vulnerability	Description
Insecure Firewall Configuration	• Misconfigured access rules allow unnecessary connections between IT and OT networks • Support teams allow excessive permissions to the management interfaces on the firewalls • Insecure firewalls propagate security threats to the OT network
OT Systems Placed within the Corporate IT Network	• Corporate systems are interconnected with the OT network to access operational data or export data to third-party management systems • OT systems such as control stations and reporting servers are placed within the IT network • Ability to use compromised IT systems to gain access to the OT network
Insufficient Security for Corporate IT Network from OT Systems	• Attacks can also originate from OT systems, then pivoting to the corporate network

COMMON OT VULNERABILITIES (CONT'D)

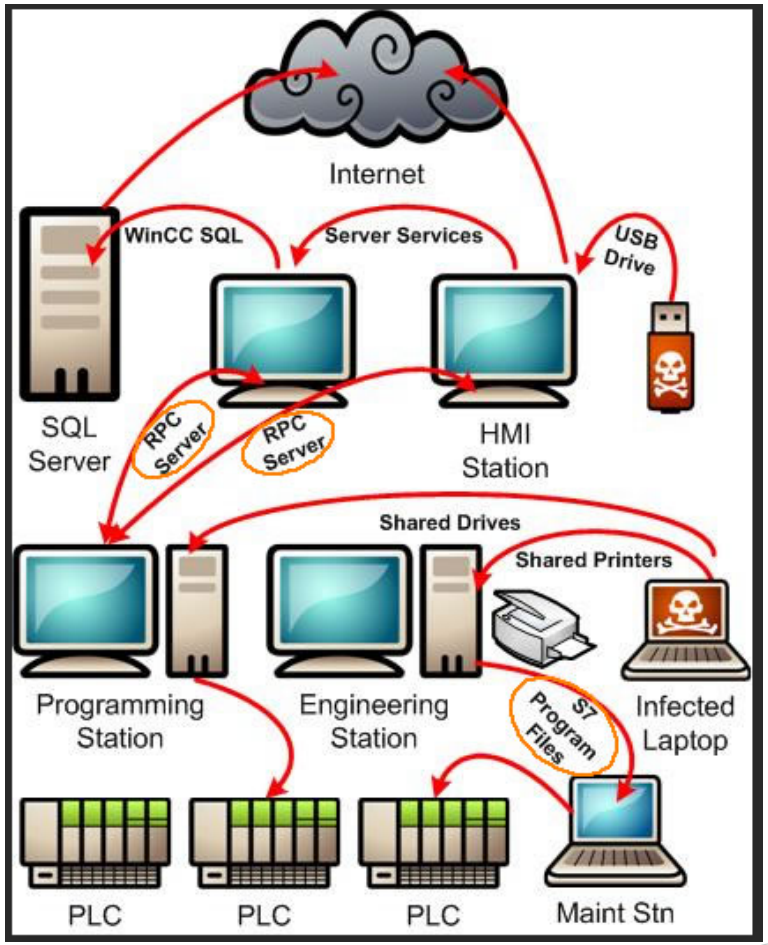
Vulnerability	Description
Lack of Segmentation within OT Networks	• Several OT networks have a flat and unsegmented configuration which assumes all systems have equal importance and functions • Compromise of a single device may expose the entire OT network
Lack of Encryption and Authentication for Wireless OT Networks	• Wi-Fi and other radio equipment in OT networks use insecure or outdated security protocols • Attackers can sniff, bypass authentication, and take over RF communications
Unrestricted Outbound Internet Access from OT Networks	• OT networks allow direct outbound network connections to support patching and maintenance from a remote location • Increased risk of malware, command-and-control, and other remote attacks

WELL-KNOWN OT ATTACKS

- Infamous OT Attacks in History

(IN)FAMOUS OT ATTACKS IN HISTORY

- Colonial Pipeline (2021)
  - Ransomware attack halted petroleum pipeline operations
  - Shuttered gas stations and grounded some commercial flights in 17 US states for a week
- Casino Database Accessed via Fish Tank (2018)
  - Attackers used an IoT-connected fish tank thermostat to exfiltrate information from the casino's High Roller database
- Kemuri Water Company* (2016)
  - Attackers accessed the water district's valve and flow control application
  - They reprogrammed PLCs to alter the number of chemicals entering the water supply, affecting water treatment and production capabilities
  - This caused water supply recovery times to increase



* Not its real name

(IN)FAMOUS OT ATTACKS IN HISTORY (CONT'D)

- Ukraine Power Grid (2016, 2015)
  - Attackers repurposed BlackEnergy3 (MS Office macro malware)
  - Corrupted Human Machine Interfaces
  - Caused monitoring stations to abruptly go blind and breakers to trip in 30 substations
  - Shut off electricity to approximately 225,000 customers
- German Steel Mill (2014)
  - Attackers gained access to the business network of the steel plant
  - They pivoted from that into the production network
  - It caused many failures of individual control systems
  - Ultimately prevented a blast furnace from shutting down in a controlled manner
  - Caused extensive damage to the plant
- New York Dam (2013)
  - Attackers gained access to a SCADA system that was connected to the Internet via a cellular modem

(IN)FAMOUS OT ATTACKS IN HISTORY (CONT'D)

- Target Stores (2013)
  - Hackers broke into a third-party that maintained Target Store's HVAC control system
  - This gave them access to the business network
  - They uploaded malicious credit card stealing software to cash registers across Target's chain of stores
- Night Dragon (2010)
  - Targeted global oil, energy, and petrochemical companies
  - Attackers collected data from SCADA systems
- Stuxnet (2010)
  - A complex worm that damaged as many as one-fifth of the nuclear power centrifuges in Iran
  - First known threat to specifically target SCADA systems in order to control networks
  - Infected servers using Windows SMB vulnerability
  - Attacked SIEMENS PLC controllers
  - Copied itself into Step 7 projects to sabotage code on the PLCs

18.10 OT ATTACK METHODOLOGY AND TOOLS

- ICS/SCADA Attack Tools
- OT Reconnaissance
- OT Penetration and Control

OT ATTACK METHODOLOGY

- Operational Technology is a very large tent encompassing a broad spectrum of device types, protocols, connectivity and processes
- OT offers many vectors for attack:
  - Internet-facing IoT devices
  - IT-OT connection
  - Diverse ICS platforms
  - Extended SCADA networking architecture
  - Physical hardware
  - Proprietary protocols
  - Un-remediated vulnerabilities in legacy systems
  - Human social engineering

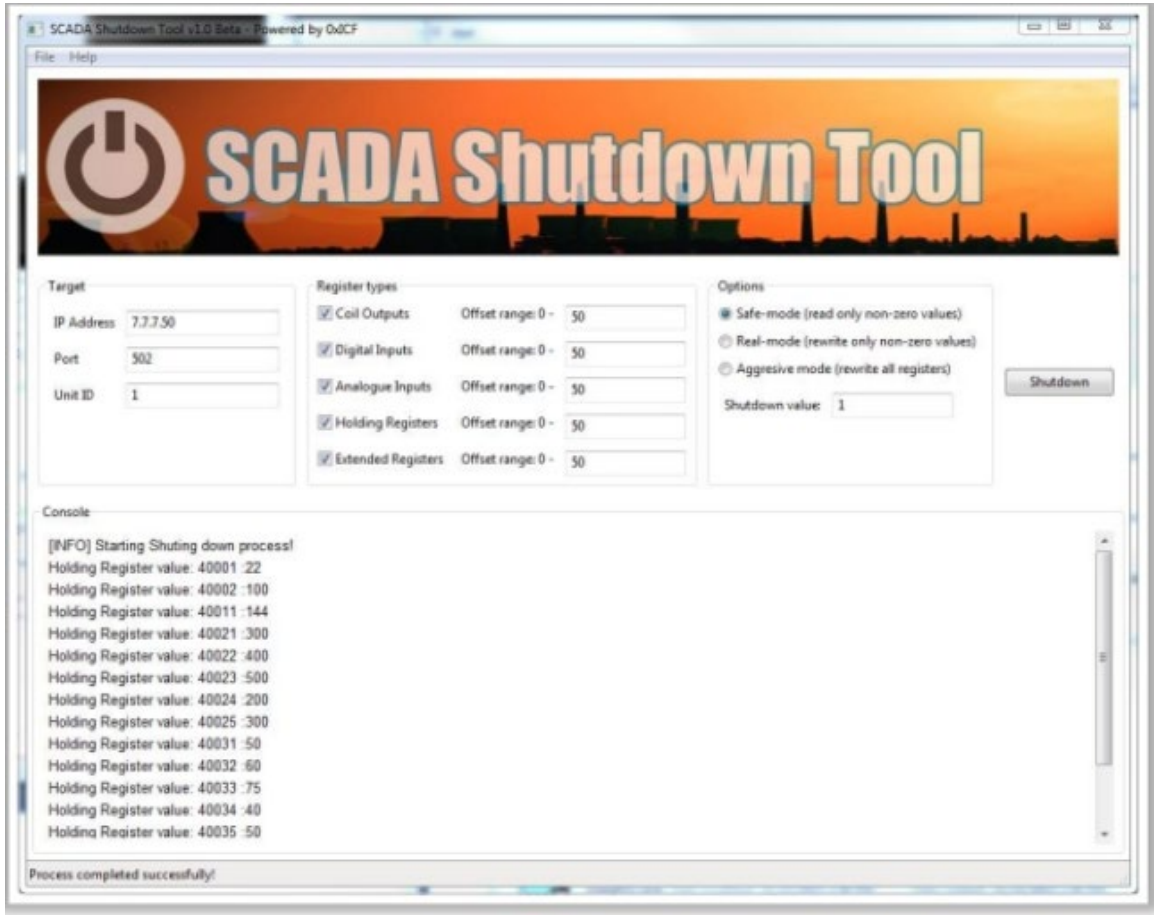
ICS/SCADA ATTACK TOOLS

- ICS Exploitation Framework / ICSSPLOIT
  - Test for PLC and ICS software vulnerabilities
- PLCinject
  - Used to inject code into PLCs
- MODBUS Penetration Testing Framework (SMOD)
  - A full-featured framework for pentesting the Modbus (PLC data communications) protocol
- Moki Linux
  - A customized version of Kali Linux geared towards ICS/SCADA pentesting professionals
- sixnet-tools
  - Tool for exploiting sixnet RTUs

All of the above-listed are available on GitHub

ICS/SCADA ATTACK TOOLS

- mbtget
  - Perl script for making modbus transactions from the command line
- SCADA Shutdown Tool
  - PLC hacking tool
  - Fuzz, scan and run remote commands
- modbus-cli
  - Read and manipulate Modbus register values
- Visit exploit.kitploit.com for additional ICS/SCADA exploits



METASPLOIT

- Has over 200 ICS and SCADA scanners and exploits

```
msf6 > search exploit scada

Matching Modules
================

   #   Name                                                                Disclosure Date  Rank       Check  Description
   -   ----                                                                ---------------  ----       -----  -----------
   0   auxiliary/admin/scada/advantech_webaccess_dbvisitor_sqli            2014-04-08       normal     Yes    Advantech WebAcc
   1   auxiliary/dos/scada/allen_bradley_pccc                                               normal     Yes    DoS Exploitation
   2   auxiliary/scanner/scada/indusoft_ntwebserver_fileaccess                              normal     No     Indusoft WebStud
   3   auxiliary/scanner/scada/sielco_winlog_fileaccess                                     normal     No     Sielco Sistemi W
   4   exploit/multi/scada/inductive_ignition_rce                          2020-06-11       excellent  Yes    Inductive Automa
   5   exploit/windows/browser/keyhelp_launchtripane_exec                  2012-06-26       excellent  No     KeyHelp ActiveX
   6   exploit/windows/browser/teechart_pro                                2011-08-11       normal     No     TeeChart Profess
   7   exploit/windows/browser/wellintech_kingscada_kxclientdownload       2014-01-14       good       No     KingScada kxClie
   8   exploit/windows/fileformat/bacnet_csv                               2010-09-16       good       No     BACnet OPC Clien
   9   exploit/windows/fileformat/scadaphone_zip                           2011-09-12       good       No     ScadaTEC ScadaPh
   10  exploit/windows/scada/abb_wserver_exec                              2013-04-05       excellent  Yes    ABB MicroSCADA w
   11  exploit/windows/scada/advantech_webaccess_dashboard_file_upload     2016-02-05       excellent  Yes    Advantech WebAcc
   12  exploit/windows/scada/advantech_webaccess_webvrpcs_bof              2017-11-02       good       No     Advantech WebAcc
   13  exploit/windows/scada/citect_scada_odbc                             2008-06-11       normal     No     CitectSCADA/Cite
   14  exploit/windows/scada/codesys_gateway_server_traversal              2013-02-02       excellent  No     SCADA 3S CoDeSys
   15  exploit/windows/scada/codesys_web_server                            2011-12-02       normal     Yes    SCADA 3S CoDeSys
   16  exploit/windows/scada/daq_factory_bof                               2011-09-13       good       No     DaqFactory HMI N
```

SEARCHSPLOIT

- Searchsploit has over 64 SCADA/ICS exploits

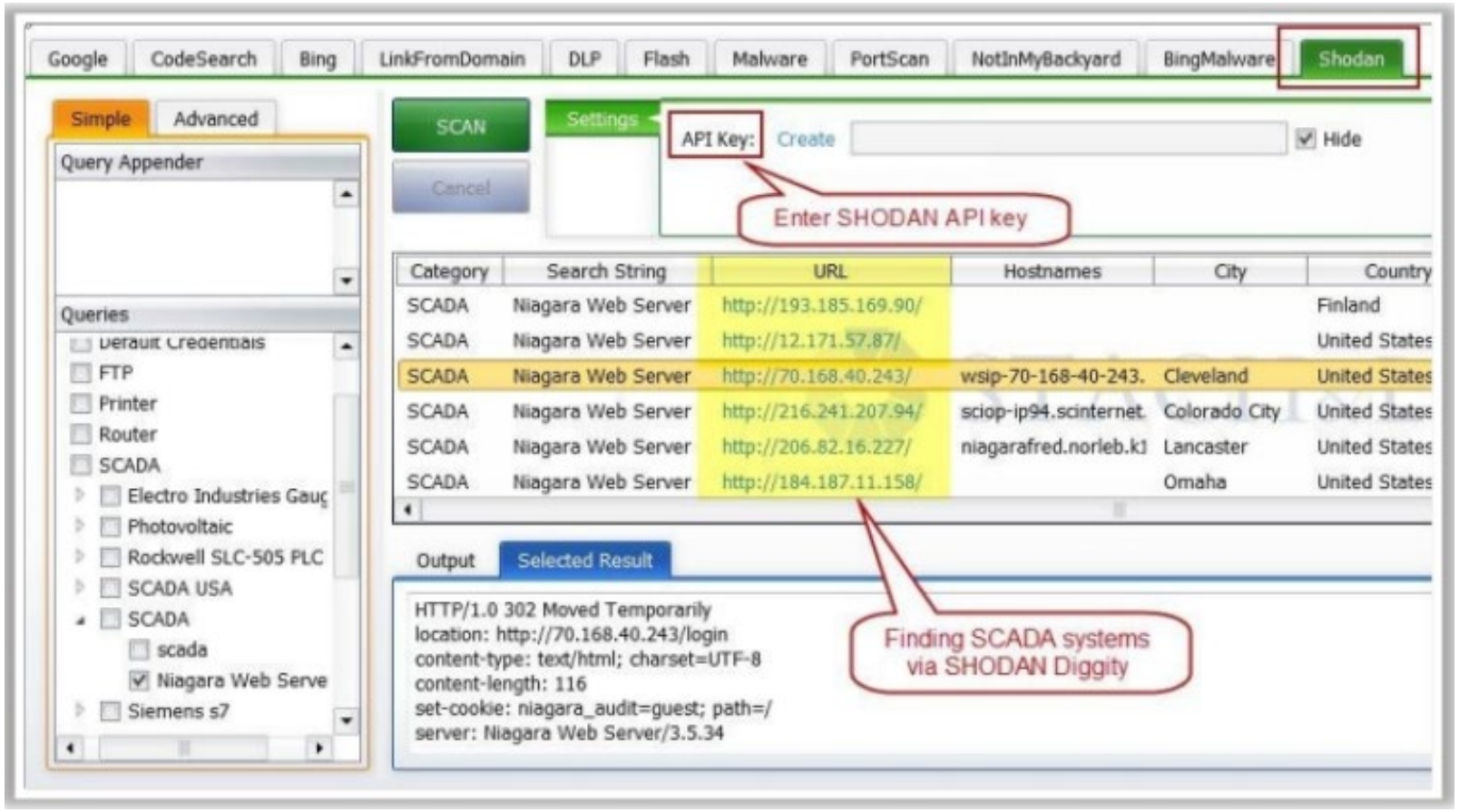
```
└─$ searchsploit scada
---------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------
ABB MicroSCADA - 'wserver.exe' Remote Code Execution (Metasploit)
Advantech Studio 7.0 - SCADA/HMI Directory Traversal
Advantech Webaccess HMI/SCADA Software - Persistence Cross-Site Scripting
Advantech WebAccess SCADA 8.3.2 - Remote Code Execution
Advantech/BroadWin SCADA Webaccess 7.0 - Multiple Vulnerabilities
BroadWin Webaccess SCADA/HMI Client - Remote Code Execution
Certec EDV atvise SCADA Server 2.5.9 - Local Privilege Escalation
CirCarLife SCADA 4.3.0 - Credential Disclosure
CitectSCADA ODBC Server - Remote Stack Buffer Overflow (Metasploit)
CitectSCADA/CitectFacilities ODBC - Remote Buffer Overflow (Metasploit)
ClearSCADA - Remote Authentication Bypass
CoDeSys SCADA 2.3 - Remote Buffer Overflow
CoDeSys SCADA 2.3 - WebServer Stack Buffer Overflow (Metasploit)
DATAC RealWin SCADA Server - Remote Buffer Overflow (Metasploit)
DATAC RealWin SCADA Server 1.06 - Remote Buffer Overflow
DATAC RealWin SCADA Server 2 - On_FC_CONNECT_FCS_a_FILE Buffer Overflow (Metasploit)
DATAC RealWin SCADA Server 2.0 (Build 6.1.8.10) - Buffer Overflow
DATAC RealWin SCADA Server 2.0 (Build 6.1.8.10) - SCPC_INITIALIZE Buffer Overflow (Metasploit)
```

OT RECONNAISSANCE

- Information Gathering
- Sniffers and Scanners

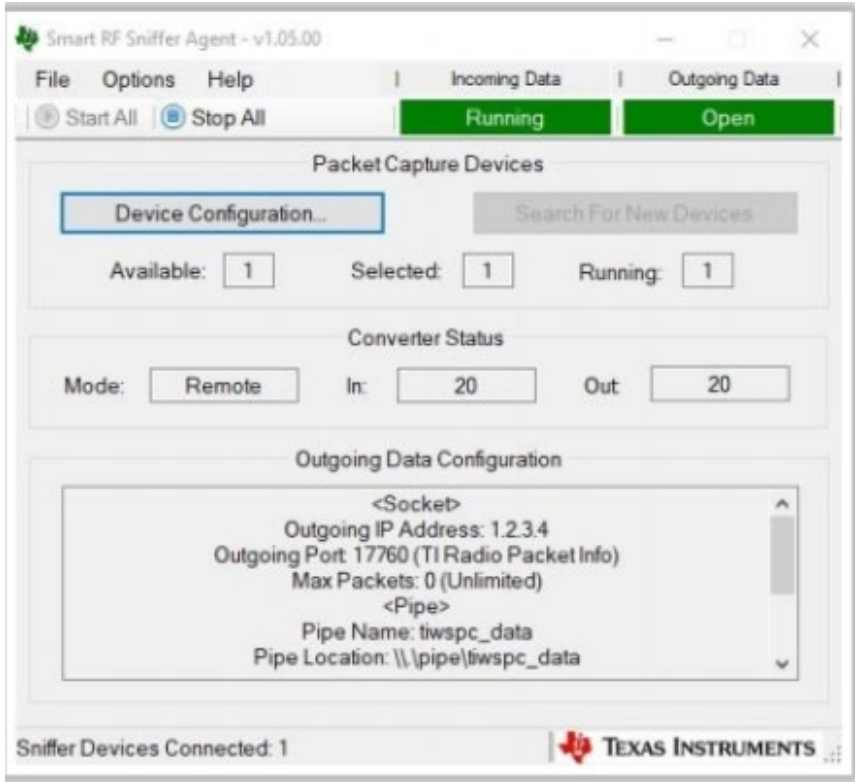
OT RECONNAISSANCE TOOLS

- Shodan.io
- SearchDiggity
- Kamerka-GUI
- Redpoint
- s7scan
- SCADAPASS
- plcscan
- nmap



SNIFFERS/VULNERABILITY SCANNERS

- Skybox
  - Detailed path analysis across OT-IT networks
  - Provides insight into vulnerabilities and attack vectors
- Nessus
  - Vulnerability scanner
- Network Miner, Wireshark
  - Passive sniffers
- GrassMarlin
  - ICS/SCADA passive network topology mapper
- SmartRF Packet Sniffer
  - Uses the CC13xx and CC26xx family of capture devices
  - Display over-the-air packets of ZigBee, EasyLink, BLE
- CyberX
  - IoT/ICS vulnerability scanner



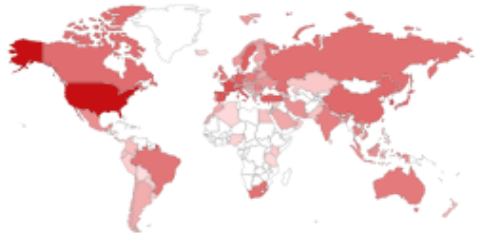
SHODAN EXAMPLE

SHODAN | Explore | Downloads | Pricing | port:502

TOTAL RESULTS

59,487

TOP COUNTRIES



United States	11,870
Korea, Republic of	4,931
France	3,067
Spain	2,665
Italy	2,619

More...

View Report | Browse Images | View on Map

New Service: Keep track of what you have connected to the Internet. Ch

49.135.37.229

UQ Communications Inc.

Japan, Yokohama

ics

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)

Unit ID: 255
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Ill...
```

182.214.231.194

LG POWERCOMM

Korea, Republic of, Seoul

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)
```

NMAP SCAN EXAMPLES

- Scan well-known ICS/SCADA ports:

```
nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p 80, 102,
443, 502, 530, 593, 789, 1089-1091, 1962, 2222, 2404, 4000,
4840, 4843, 4911, 9600, 19999, 20000, 20547, 34962-34964, 34980,
44818, 46823, 46824, 55000-55002 <target IP>
```

- Identify HMI Systems

```
nmap -Pn -sT -p 46824 <target IP>
```

- Scan Siemens SIMATIC S7 PLCs:

```
nmap -Pn -sT -p 102 --script w7-info <target IP>
```

- Scan Modbus Devices:

```
nmap -Pn -sT -p 502 --script modbus-discover <target IP>
```

NMAP SCAN EXAMPLES (CONT'D)

- Scan BACnet Devices:

```
nmap -Pn -sU -p 47808 --script bacnet-info <target IP>
```

- Scan Ethernet/IP Devices:

```
nmap -Pn -sU -p 44818 --script enip-info <target IP>
```

- Scan Niagra Fox Devices:

```
nmap -Pn -sT -p 1911,4911 --script fox-info <target IP>
```

- Scan ProConOS Devices:

```
nmap -Pn -sT -p 20547 --script proconos-info <target IP>
```

- Scan Omron PLC Devices:

```
nmap -Pn -sT -p 9600 --script omron-info <target IP>
```

- Scan PCWorx Devices:

```
nmap -Pn -sT -p 1962 --script pcworx-info <target IP>
```

COMMON PLC TCP PORTS BY PRODUCT

- Allen Bradley – Newer Rockwell PLCs : 44818
- Allen Bradley – Older Rockwell PLCs: TCP 2222
- BECKHOFF Embedded PC: 48898
- C-more HMI Programming: 9999
- Danfoss ECL Apex: 5050
- FATEK FB Series: 500
- GE Fanus Series 90-30: 18245
- GE SRTP uses TCP ports 18245 and 18246
- GE QuickPanels use TCP port: 57176
- HITACHI EHV Series: 3004
- KEYENCE KV-5000: 8501
- Korenix 6550: 502
- Koyo Ethernet: 28784
- LS GLOFA FEnet: 2004
- LS XGB FEnet: 2004
- LS XGK FEnet: 2004
- Memobus (Yaskawa MP Series Controllers): 502
- Mitsubishi FX: 1025
- MITSUBISHI FX3u (Ethernet): 5001
- MITSUBISHI MELSEC-Q (Ethernet): 4999
- MITSUBISHI MR-MQ100 (Ethernet): 4999
- MITSUBISHI QJ71E71 (Ethernet): 5002
- MODBUS TCP/IP (Ethernet): 502
- MODBUS Server (Modbus RTU Slave): 502

COMMON PLC TCP PORTS BY PRODUCT (CONT'D)

- Omron PLC: 9600
- Panasonic FP (Ethernet): 9094
- Panasonic FP2 (Ethernet): 8500
- Parker Drives using MODBUS TCP/IP (Ethernet): 502
- Red Lion HMI's: 789
- SAIA S-BUS (Ethernet): 5050
- Schleicher XCX 300: 20547
- Siemens S7 protocol uses TCP port: 102
- Toshiba Series PLC's uses Modbus port: 502
- Trio (MODBUS RTU, TCP/IP): 502
- Unitronics Socket1 – TCP slave: 20256
- Unitronics Socket2 – TCP slave: 502
- Unitronicsw Socket3 – TCP slave: 20257
- Wago CODESYS – TCP: 2455
- YAMAHA NETWORK BOARD Ethernet RCX series uses telnet port: 23
- YASKAWA MP Series Ethernet: 10000
- YASKAWA MP2300Siec: 44818
- YASKAWA SMC 3010 (Ethernet): 23
- Yokogawa FA-M3 (Ethernet): 12289

OT PENETRATION AND CONTROL

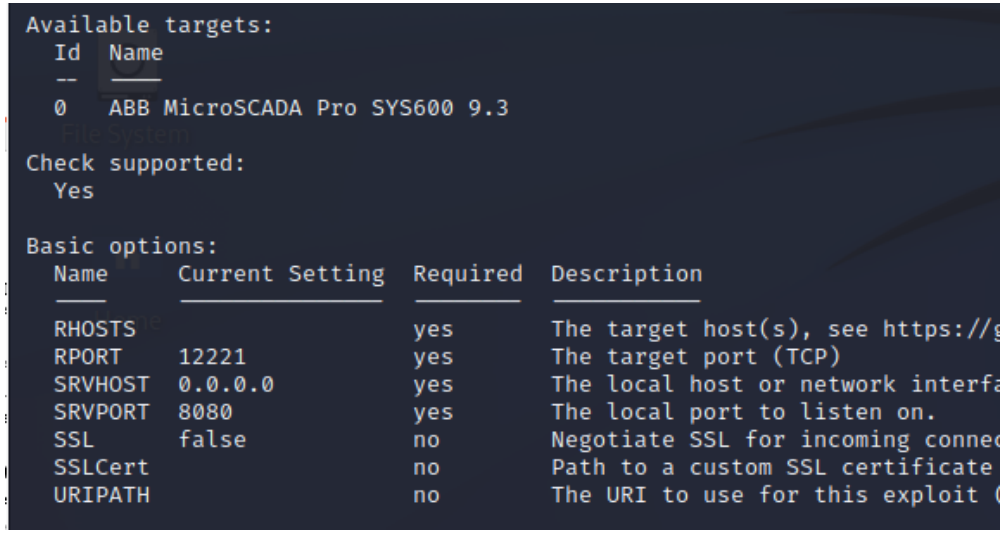
- Common Attacks

COMMON OT ATTACKS

- OT is subject to all IoT attacks
  - and many of the same attacks on regular IT networks
- Spear Phishing
- Unauthorized access
- Password cracking
- Malware / Trojans / Bots
- Protocol Abuse
- Potential Destruction of Resources
- Denial-of-Service
- Side-channel attacks
- Hardware-specific attacks

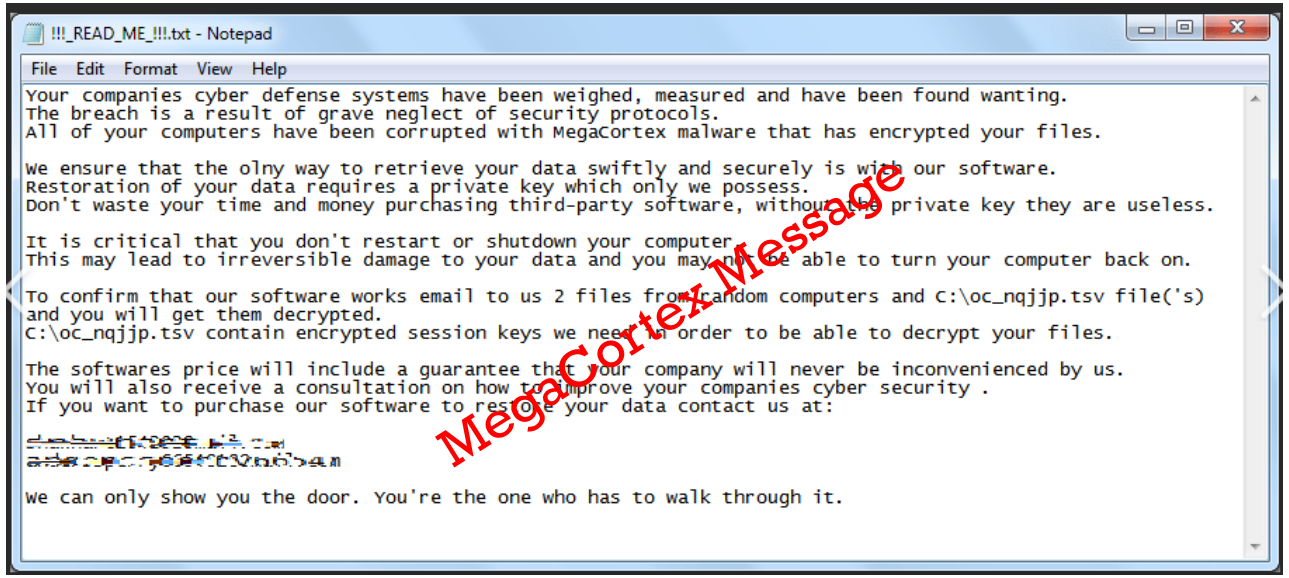
OT ATTACK TOOLS

- MITRE ATT&CK lists 79 techniques for attacking ICS
  - https://attack.mitre.org/techniques/ics/
- Metasploit lists 72 modules to attack ICS/SCADA
  - 18 exploits with a rank of great or excellent
- GitHub lists about a dozen ICS/SCADA/PLC/RTU exploits
- Exploit-DB lists 25 verified SCADA exploits
- Shodan.io returns:
  - 2700+ results for ICS
  - 1300+ results for SCADA



OT FILELESS MALWARE

- MegaCortex
  - Fileless OT ransomware
  - Distributed by Qakbot (Qbot), Emotet, or Reitspoof trojan
  - Uses PsExec to execute malicious commands
- Other Fileless OT Malware:
  - Disruptionware
  - LockerGoga
  - Triton
  - Olympic Destroyer
  - SamSam
  - Shamoon3
  - VPNFilter
  - Havex

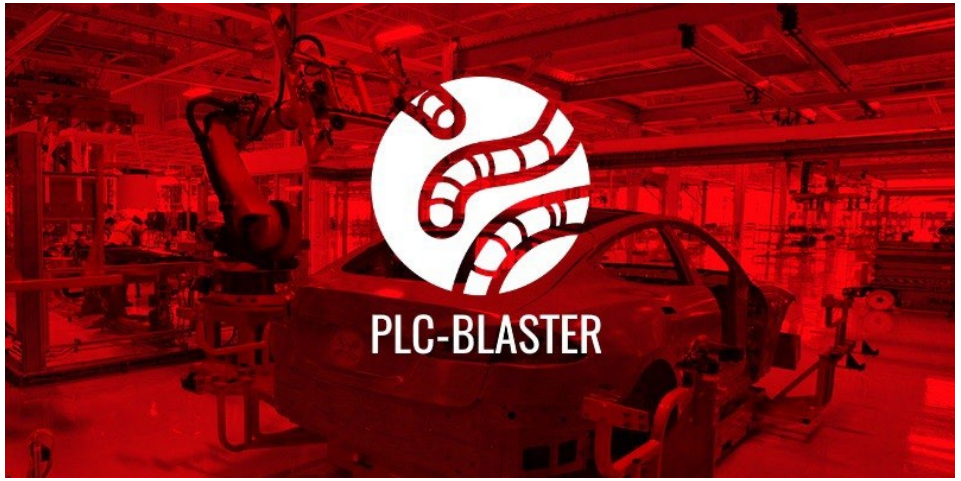


HMI ATTACKS

- HMI is the local control station a human operator uses to manage a particular ICS/SCADA device
- OS is typically:
  - Windows IoT Core
  - Linux Core
- It is especially subject to:
  - Memory Corruption
  - Credential Management
  - Lack of Authentication/Authorization
  - Insecure Defaults
  - Code Injection

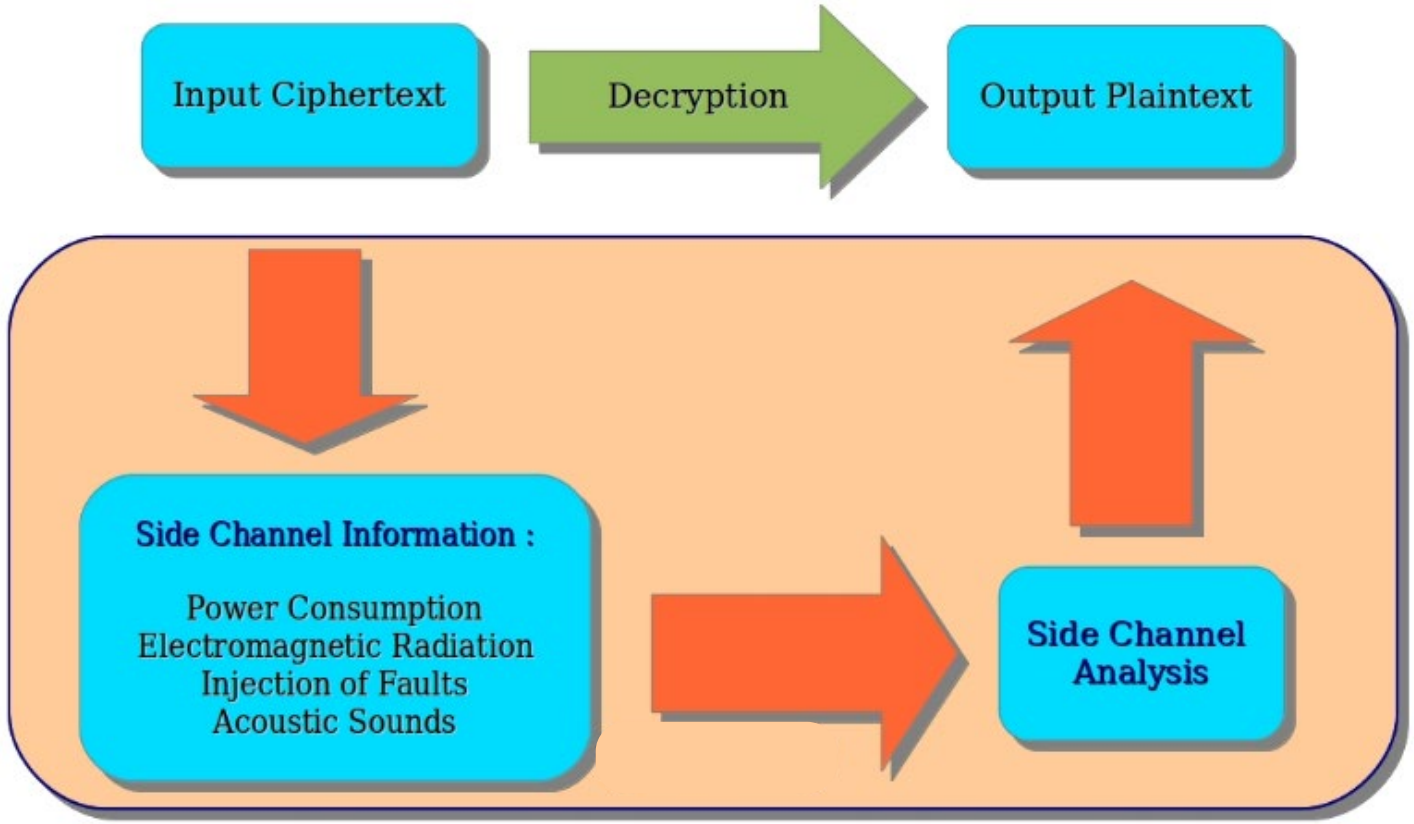
PLC ATTACKS

- PLC Rootkit Attack
- PLC code tampering
- Payload sabotage attacks
- Worms and Trojans such as:
  - PLC Blaster
    - Siemens S7 PLCs
    - TCP 102
  - Stuxnet
    - Considered the first cyber weapon
    - Destroys uranium enrichment centrifuges by causing them to spin erratically
    - Targeted attack causing extensive damage to Iran's nuclear program
    - https://github.com/loneicewolf/Stuxnet-Source

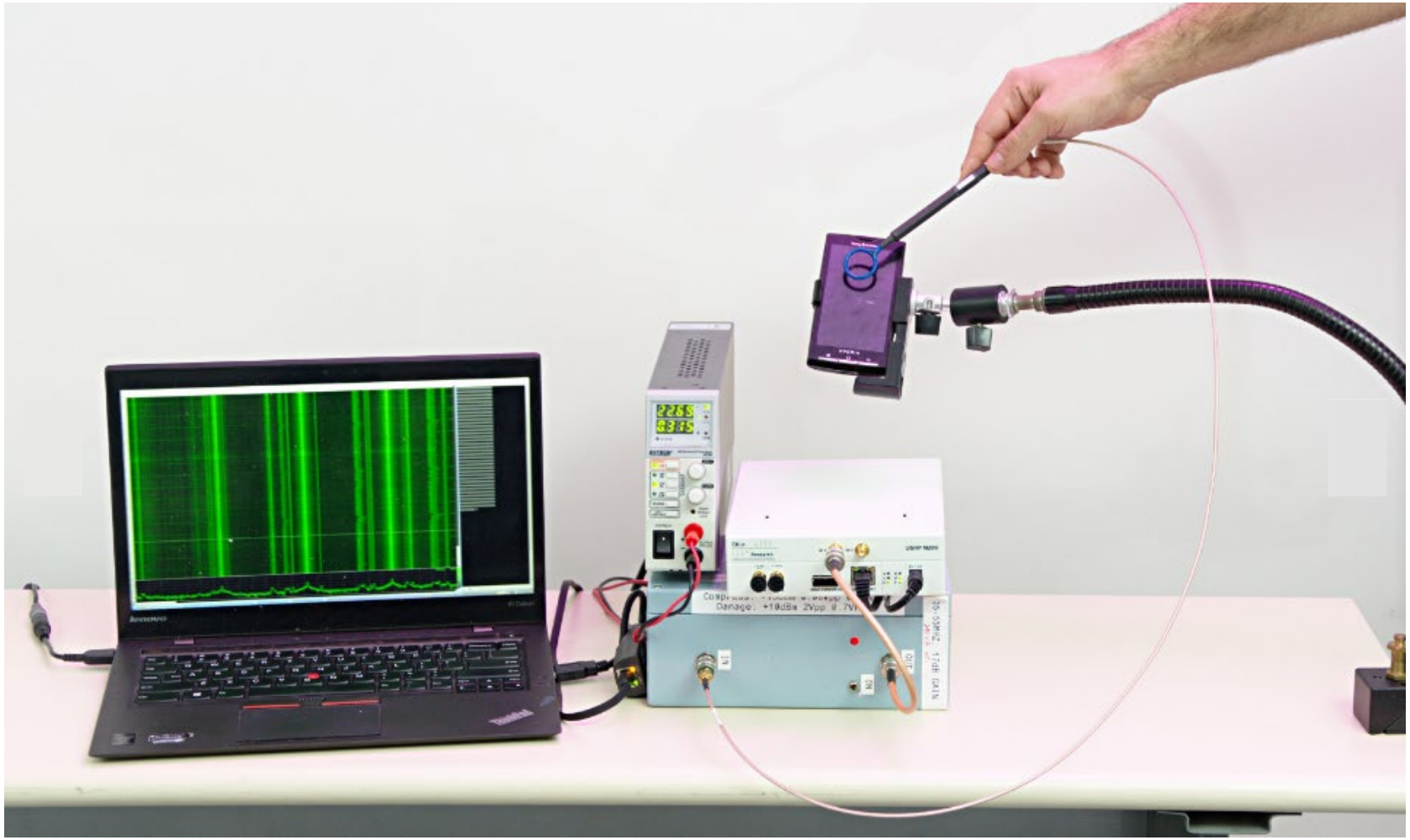


SIDE-CHANNEL ATTACKS

- Timing Analysis
- Power Analysis

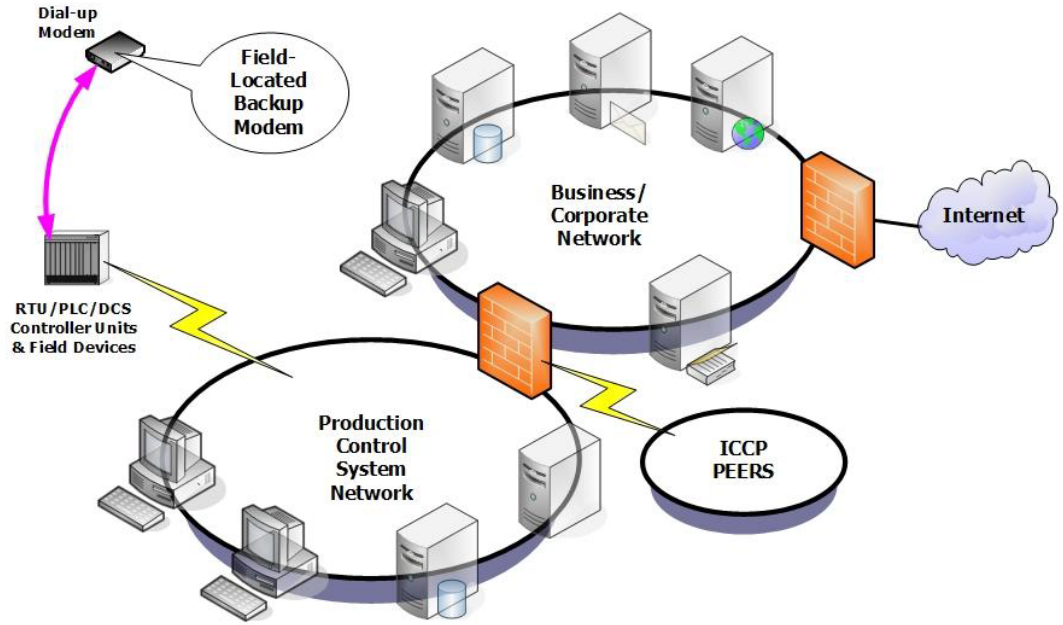


SIDE-CHANNEL ATTACK EXAMPLE



RTU ATTACKS

- Direct dial to RTU modems
  - Most have default or no authentication
  - Most will identify themselves on answer
    - Attacker can then research and use its commands
- Target Modbus communications
  - Crafted Modbus/TCP packet exceeding MTU of 260 bytes can cause DoS
  - Clear text makes it easy to sniff
- Target update packages



CRITICAL RTU ATTACK EXAMPLES

- CVE-2019-14931
  - Unauthenticated remote OS Command Injection
  - Complete CIA compromise
  - Mitsubishi Electric ME-RTU devices through 2.02
  - INEA ME-RTU devices through 3.0
  - CVSS 10.0
- CVE-2017-12739
  - Unauthenticated RCE
  - Siemens SICAM RTUs SM-2556 COM Modules
  - Integrated web server (port 80/tcp) of the affected devices could allow unauthenticated remote attackers to execute arbitrary code on the affected device
  - CVSS 10.0

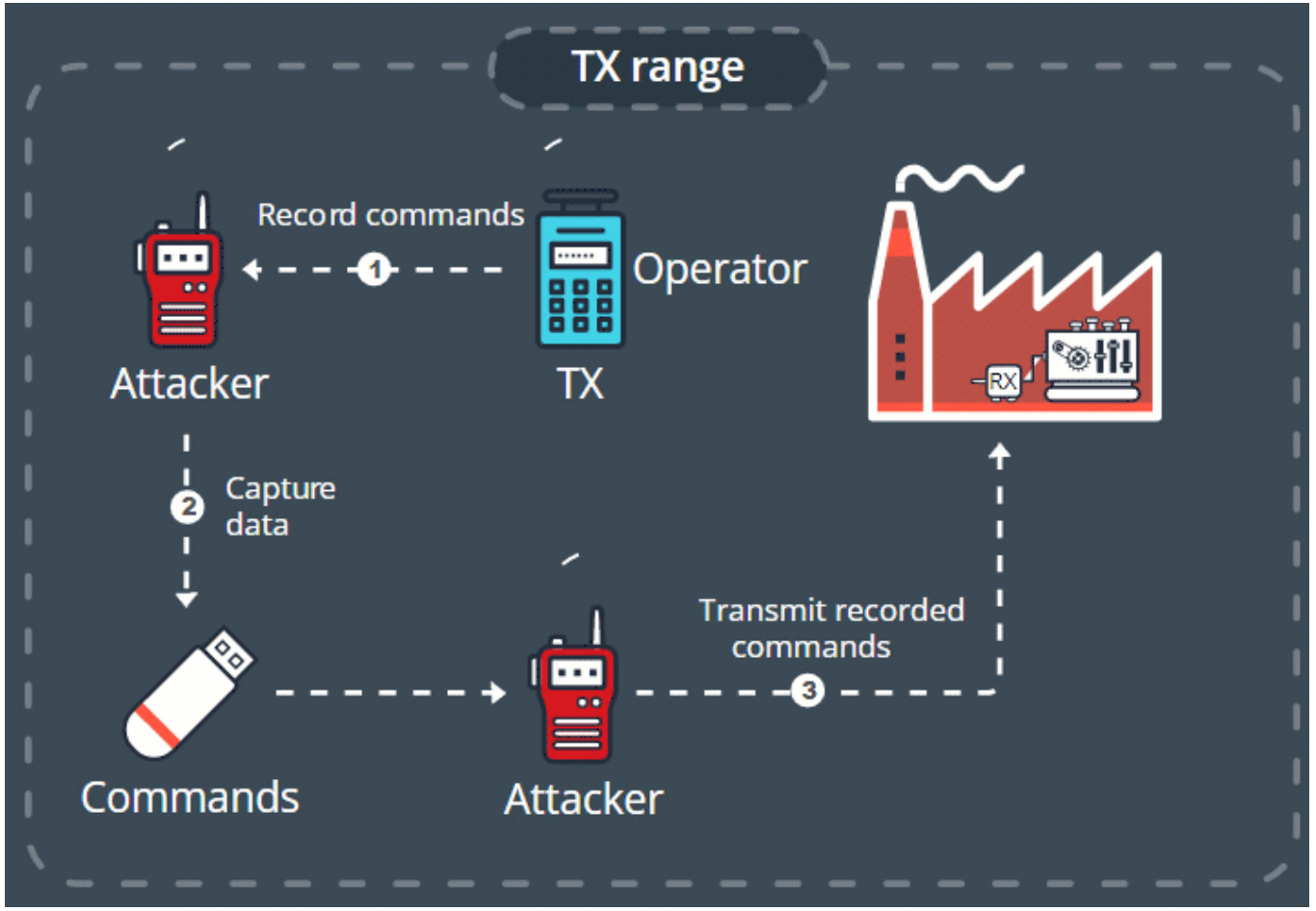
RF CONTROL HACKING

- Radio frequency (RF) protocols are often used to control industrial machines
- Used for simple operations such as turning on a motor (drills), lifting a load (cranes), or maneuvering a heavy-duty vehicle
- They use fixed codes that can be sniffed and replayed
- CVE-2018-17935, CVE-2018-19023: Authentication Bypass by Capture-Replay
- CVSS 8.1

RF REMOTE CONTROL ATTACK TYPES

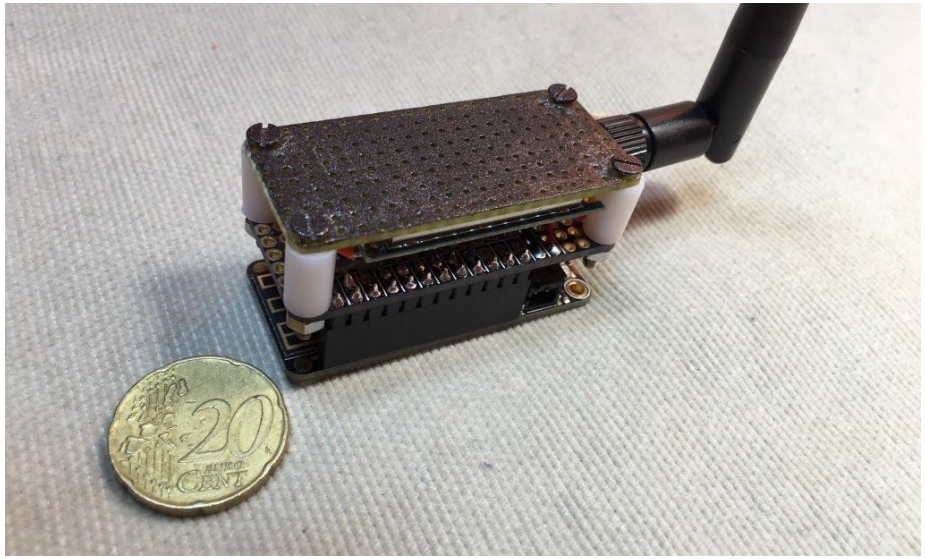
- Replay Attack
- Command Injection/command spoofing
- Abusing Emergency Stop (E-stop)
  - An attacker can replay emergency stop commands indefinitely to engage a persistent denial-of-service condition
  - It's also possible for an attacker to turn a machine back on, even though the operator issued an emergency stop
- Re-pairing with Malicious RF Controller
- Cloning a remote controller
- Malicious Reprogramming Attack
- DDoS

RF REMOTE CONTROL EXAMPLE



RFQUACK

- Practical POC for RF Control Attacks
- Battery-powered, pocket-sized embedded device for remote access
- Attacker gains temporary physical access to the facility
- Hides device in an inconspicuous place
- Device must be in RF range of the machines
- Device is remote controlled by the attacker
- Built by TrendMicro researchers (2019)



18.11 OT HACKING COUNTER MEASURES

- UEBA
- ICS/SCADA Protection
- Countermeasures
- Tools

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA)

- ICS, SCADA, and IoT devices often run proprietary, inaccessible, or unpatchable operating systems
- Traditional tools used to detect the presence of malicious cyber activity in normal enterprise networks will not function properly
- User and entity behavior analytics (UEBA) is best suited to detect and classify known-good behavior from these systems to create a baseline
  - Once a known-good baseline is established, deviations can be detected and analyzed
  - May be heavily dependent on artificial intelligence and machine learning
  - May also have a higher false-positive rate
- UEBA is now evolving into Extended Detection and Response (XDR)
- Tools include:
  - Rapid7 InsightIDR
  - Splunk
  - Aruba IntroSpect.

CONSIDERATIONS FOR APPLYING ANTIVIRUS UPDATES AND PATCHING

- A SCADA workstation might be isolated from the internet
- Infections are often caused by removable media
- Once the system is cleaned, any anti-malware solution will need to be manually updated to ensure it has the latest virus definitions
- The same goes for applying security patches
- Without the latest virus definitions or patches, the system can easily become re-infected.

ICS/SCADA PROTECTION RECOMMENDATIONS

As recommended by the US Dept of Energy, CISA, NSA, and FBI:

- Isolate ICS/SCADA systems and networks from corporate and Internet networks
  - Use strong perimeter controls
  - Limit any communications entering or leaving ICS/SCADA perimeters.
- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible
- Have a cyber incident response plan
  - Exercise it regularly with stakeholders in IT, cybersecurity, and operations.

ICS/SCADA PROTECTION RECOMMENDATIONS (CONT'D)

- Change all passwords to ICS/SCADA devices and systems on a consistent schedule
- Ensure Open Platform Communications / Unified Architecture (OPC UA) security is correctly configured
  - Application authentication enabled
  - Explicit trust lists
- Ensure the OPC UA certificate private keys and user passwords are stored securely
- Maintain known-good offline backups for faster recovery upon a disruptive attack
  - Conduct hashing and integrity checks on firmware and controller configuration files to ensure backup validity.

ICS/SCADA PROTECTION RECOMMENDATIONS (CONT'D)

- Limit ICS/SCADA systems' network connections to only specifically allowed management and engineering workstations
- Robustly protect management systems by configuring:
  - Device Guard
  - Credential Guard
  - Hypervisor Code Integrity (HVCI)
- Install Endpoint Detection and Response (EDR) solutions on these subnets
- Ensure strong anti-virus file reputation settings are configured
- Implement robust log collection and retention from ICS/SCADA systems and management subnets.

ICS/SCADA PROTECTION RECOMMENDATIONS (CONT'D)

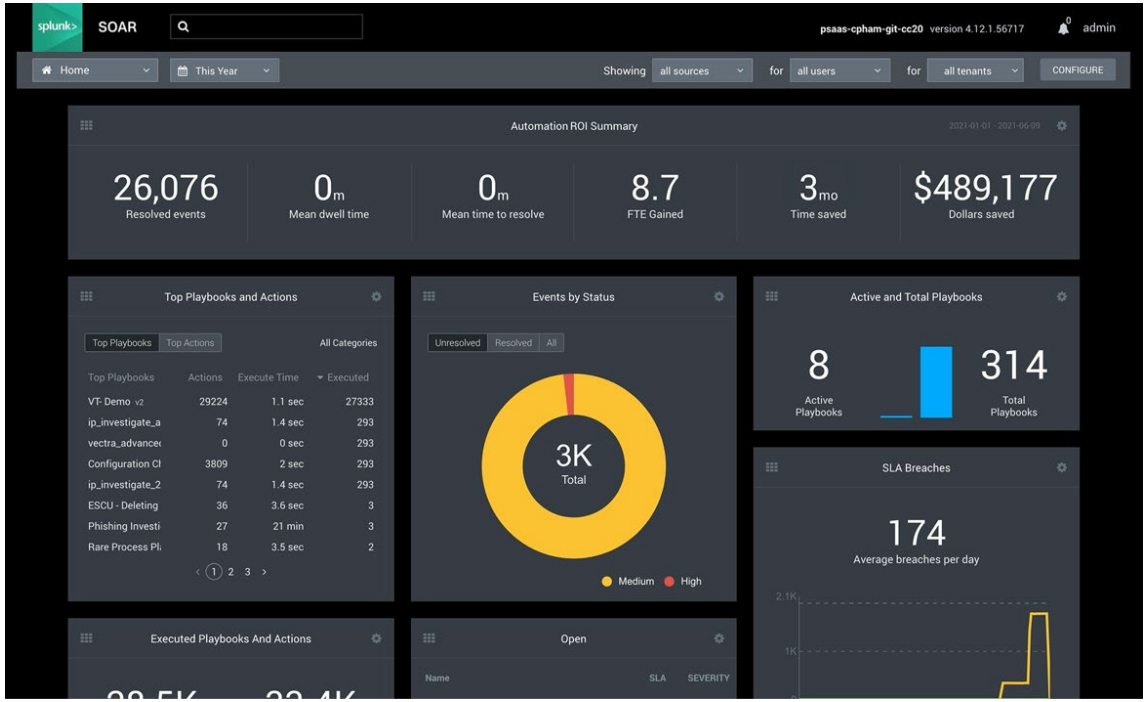
- Leverage a continuous OT monitoring solution to alert on malicious indicators and behaviors
  - Watch internal systems and communications for known hostile actions and lateral movement
  - For enhanced network visibility to potentially identify abnormal traffic, consider using CISA's open-source Industrial Control Systems Network Protocol Parsers (ICSNPP)
- Ensure all applications are only installed when necessary for operation
- Enforce principle of least privilege. Only use admin accounts when required for tasks, such as installing software updates.
- Investigate symptoms of a denial of service or connection severing
  - These exhibit as delays in communications processing, loss of function requiring a reboot, and delayed actions to operator comments as signs of potential malicious activity
- Monitor systems for loading of unusual drivers, especially for ASRock driver if no ASRock driver is normally used on the system.

OT SECURITY BEST PRACTICES

- Implement a dedicated VPN gateway, or jump-host, within the enterprise DMZ
  - This should be the only access point into the plant environment for remote users
  - Remote access should never be enabled by default.
- Implement a default "deny all" access policy across the external-to-internal communication boundary
- Establish remote access multi-factor authentication (MFA) where possible
- Implement enhanced logging and monitoring:
  - across the IT/OT boundary
  - For any highly critical assets within the OT environment
  - This helps you identify traffic from rogue devices that may have gained access to the OT network.
- Implement network micro-segmentation
  - Physical air-gapping
  - Separate VLANs for distinct groups of assets
  - Reduces the risk of wide-scale compromise.

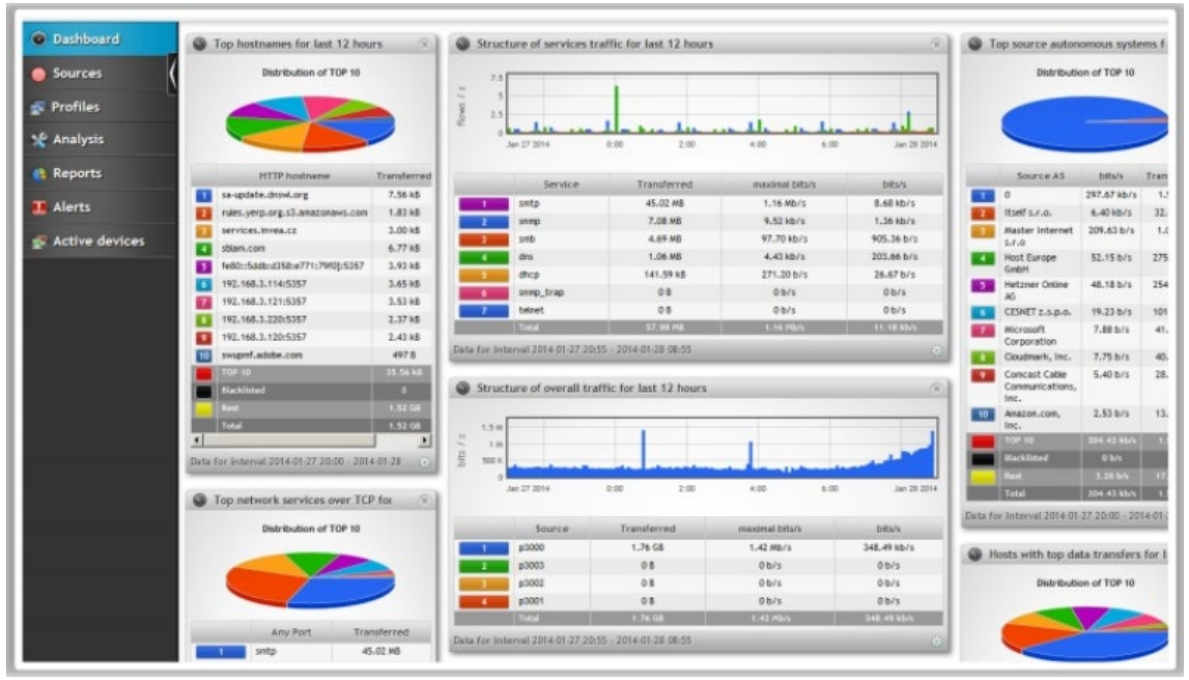
IDS/IPS FOR OT

- ICS/SCADA machines utilize very specific commands to control equipment
- You could set up strict IDS/IPS rules to detect and prevent unknown types of actions from being allowed to occur
- Tools include:
  - Splunk
  - AlienVault SIEM
  - Dragos
  - McAfee
  - Security Onion
  - Nessus



OT SECURITY TOOLS

- Indegy Industrial Cybersecurity Suite
- Tenable Industrial Security
- Flowmon
- Singtel
- Forescout
- PA-220R

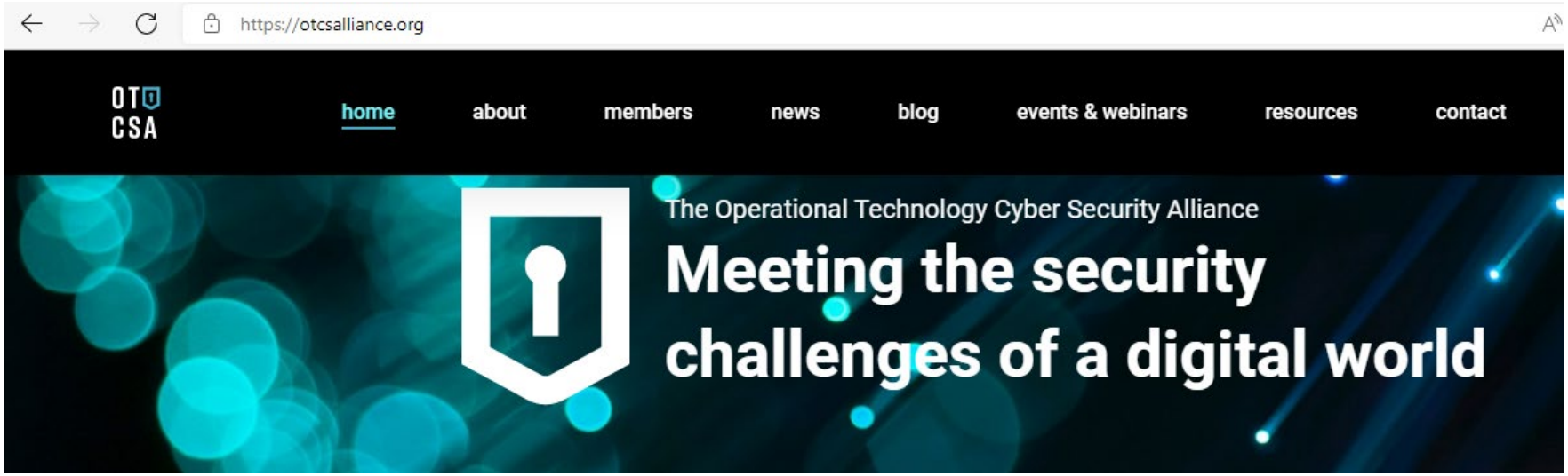


IOT/OT MONITORING TOOLS

- (Princeton) IoT Inspector
  - Open source tool to watch network interactions of your SOHO/Home IoT devices
  - Currently under major revision - re-launch slated for Spring 2023
  - https://inspector.engineering.nyu.edu/
- Domotz
  - Remote monitoring and management
- Splunk Industrial for IoT
  - Monitoring and problem root cause analysis
- Datadog IoT Monitoring
  - Performance and security monitoring
- TeamViewer IoT
  - Remote monitoring and management
- AWS IoT Device Management
  - Cloud-based IoT monitoring and management

OT SECURITY ORGANIZATIONS

- Operation Technology Cybersecurity Alliance (www.otcsalliance.org)
- Operational Technology Information Sharing and Analysis Center (www.otisac.org)
- International Operational Technology Security Association (iotsa.org).

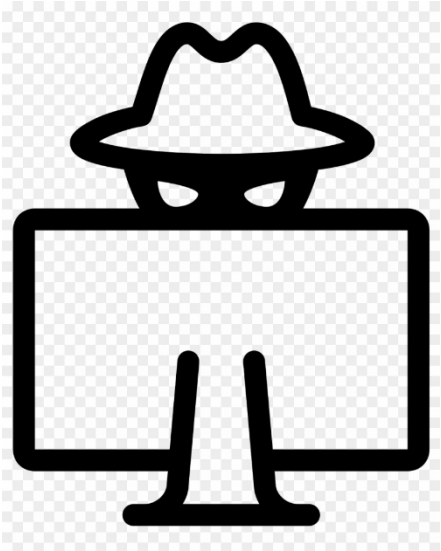


18.12 IOT AND OT HACKING REVIEW

- IoT Review
- OT Review

IOT HACKING REVIEW

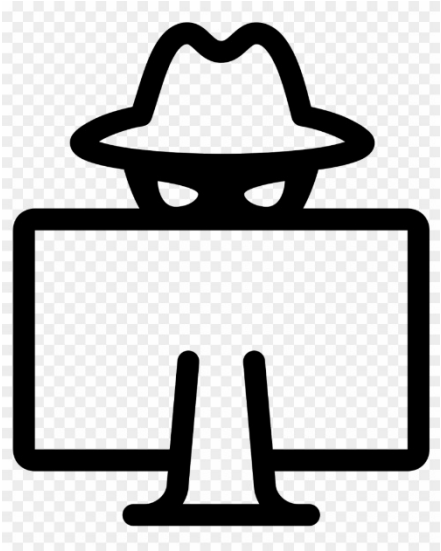
- The Internet of Things refers to everyday devices that:
  - Can connect to a network to transmit data
  - Are not considered traditional computers
- IoT devices can use a very wide range of networking protocols and transmission types
  - Most use some form of wireless communication (Bluetooth, Cellular, Zigbee/Z-Wave, Wi-Fi)
- The vast majority of IoT devices are:
  - Purpose-built for a specific task
  - Smaller, with few security controls



- IoT devices may or may not use IP addresses
  - They may use MAC addresses or some other identifier
- IoT hacking can include:
  - Physically or logically attacking the device itself
  - Intercepting, modifying, spoofing or replaying its transmissions
  - Attacking the phone/web/router app that it connects to
  - Connecting to unsecured devices that are directly exposed to the Internet.

OT HACKING REVIEW

- OT is a subset of IoT
- It is the hardware and software that monitors or controls industrial equipment, assets, and processes
- Unlike IT attacks that steal data, OT attacks tend to focus on industrial control systems (ICS and SCADA)
- OT attacks can not only shut down company equipment that affects only a company, but some equipment can be connected to and affect human life
- Both IoT and OT present a new, uncharted frontier in cyber security



- OT uses security zones to keep the business IT network separate from the manufacturing/industrial network
  - Ideally there should be no connection between the two
  - Attackers can compromise either network, and then pivot to the other network
- OT components include IIoT, ICS, SCADA, DCS, RTU, PLC, BPCS and SIS
- OT's biggest challenge is that ICS and SCADA systems are difficult to retrofit with modern security
- OT countermeasures should include all of the typical ones used to protect IoT and IT, as well as OT device-specific vulnerabilities.