



Ethical Hacking Essentials (EHE)

Master of Science in Cybersecurity

1



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023

Module 10

IoT and OT Attacks and Countermeasures

Module Objectives



- 1 Understanding IoT Concepts
- 2 Understanding IoT attacks and IoT attack Tools
- 3 Overview of IoT Attack Countermeasures and Security Tools
- 4 Understanding OT Concepts
- 5 Understanding OT Attacks and OT Attack Tools
- 6 Overview of OT Attack Countermeasures and Security Tools

IoT Attacks

Module Flow

1

Understand IoT Concepts

2

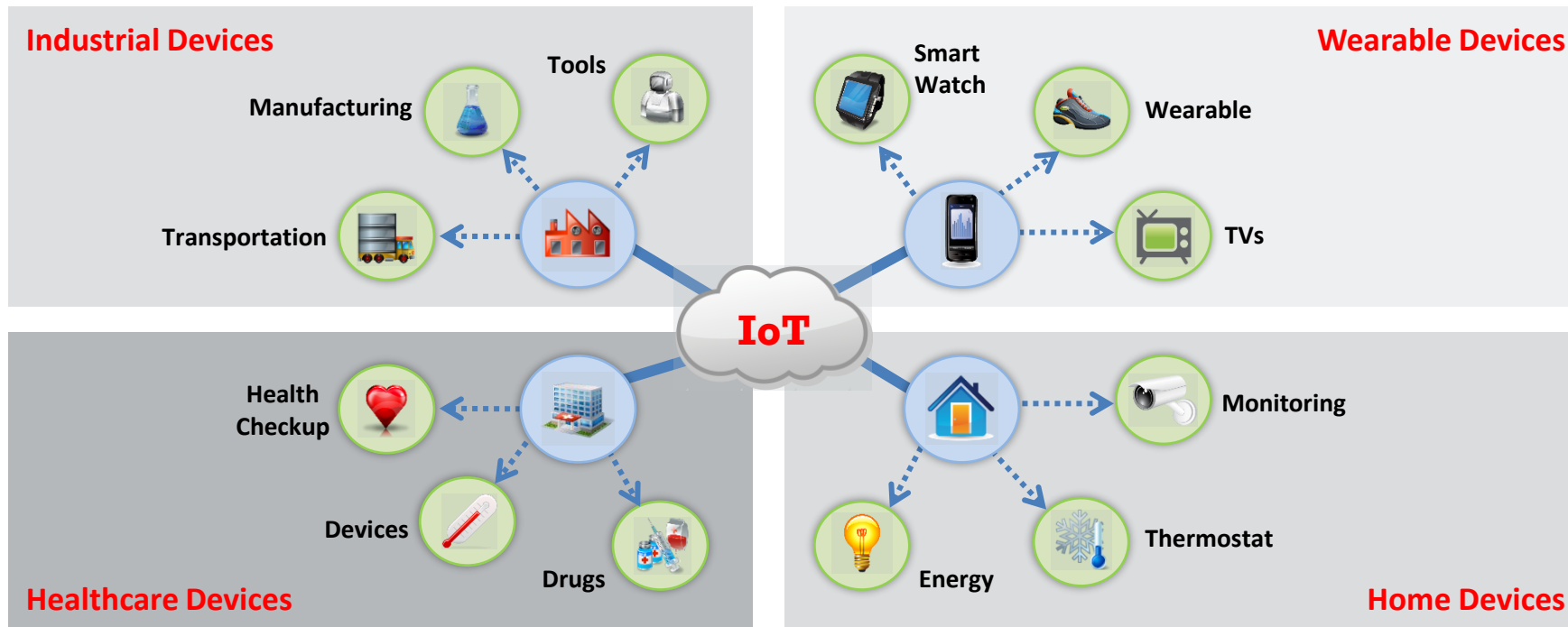
Discuss IoT Threats and Attacks

3

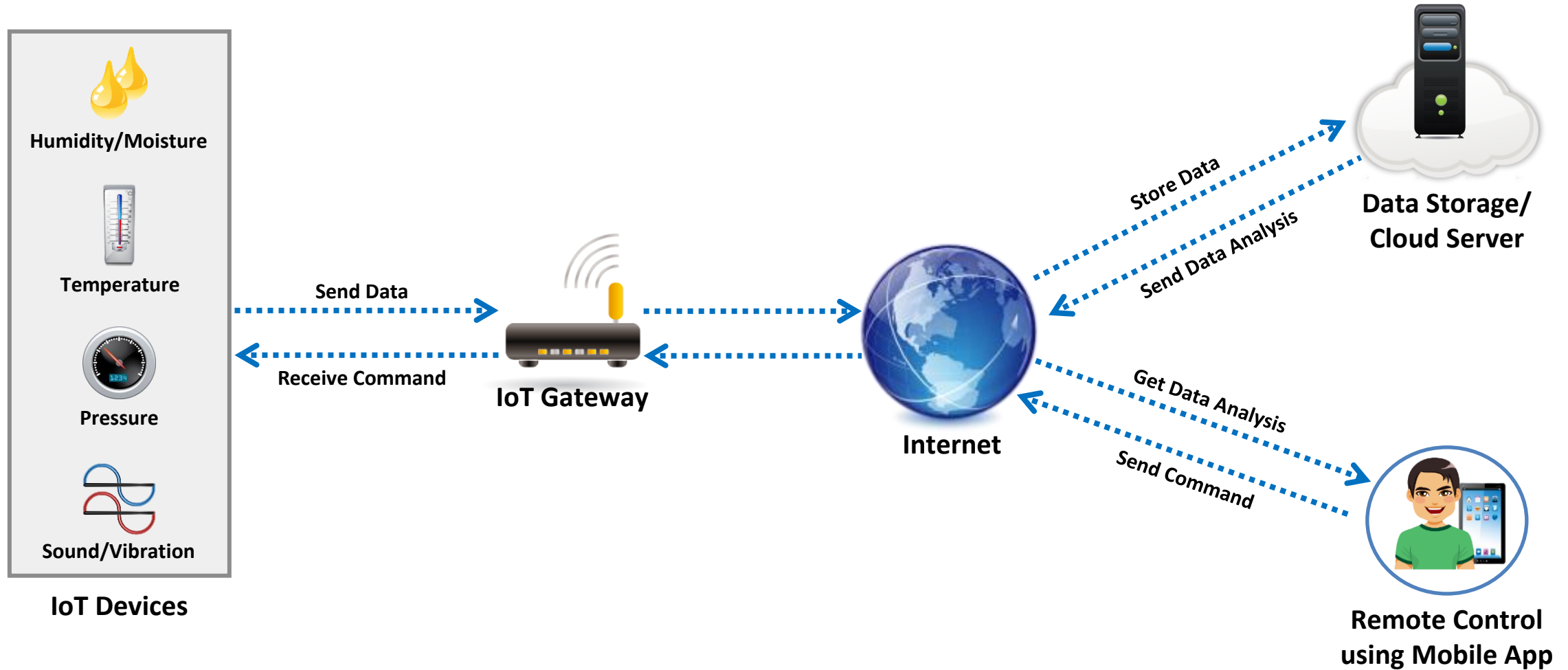
Discuss IoT Attack Countermeasures

What is IoT?

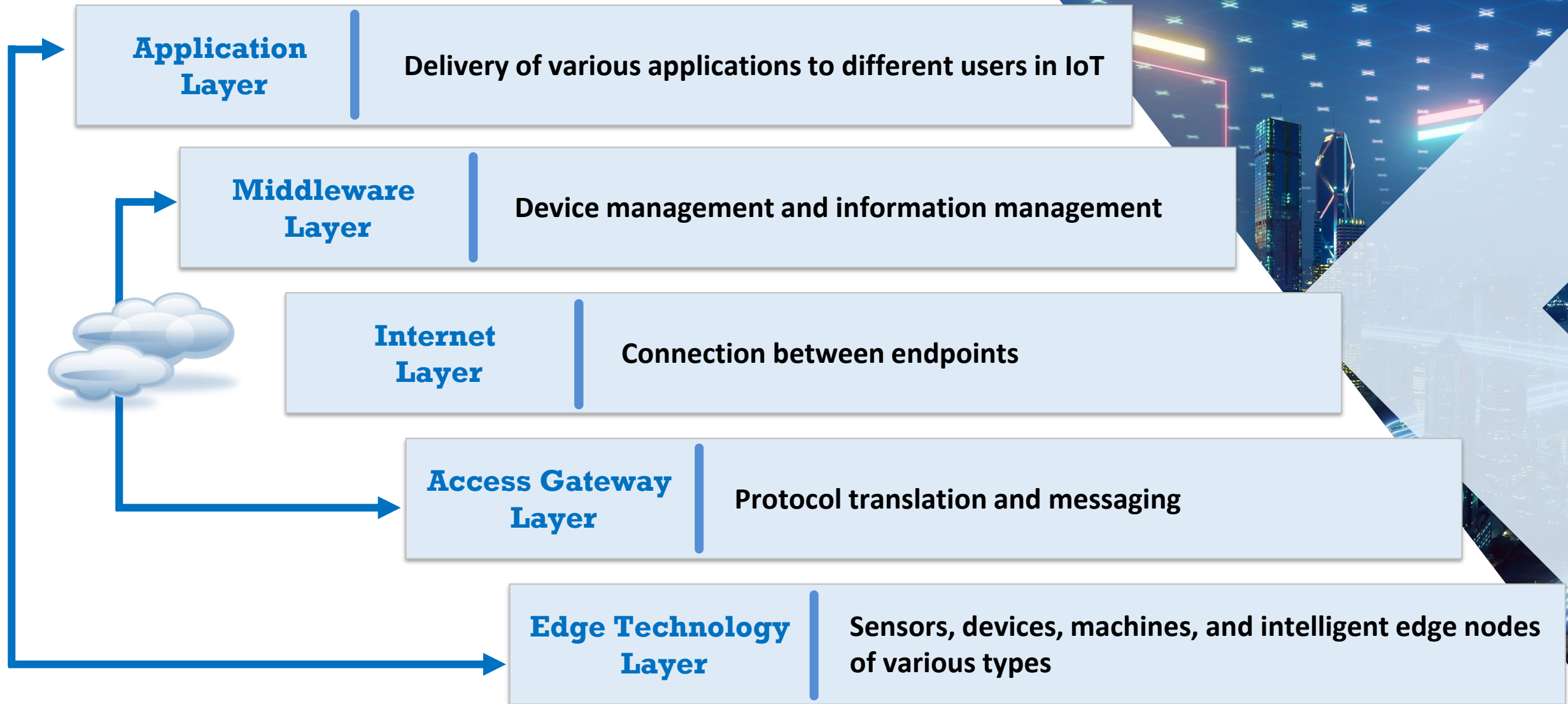
- ❑ Internet of Things (IoT), also known as **Internet of Everything** (IoE), refers to the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors.
- ❑ In IoT, the term **thing** is used to refer to a device that is **implanted on natural, human-made, or machine-made** objects and has the functionality of **communicating over the network**.



How the IoT Works



IoT Architecture



IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	• Commercial/Institutional	• Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	• Industrial	• Process, Clean Room, Campus	
Energy	• Supply/Demand	• Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	• Alternative	• Solar Wind, Co-generation, Electrochemical	
	• Oil/Gas	• Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	• Infrastructure	• Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	• Awareness & Safety	• Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	• Convenience & Entertainment	• HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	• Care	• Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	• In Vivo/Home	• Implants, Home, Monitoring Systems	
	• Research	• Drug Discovery, Diagnostics, Labs	
Transportation	• Non-Vehicular	• Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	• Vehicles	• Consumer, Commercial, Construction, Off-Highway	
	• Trans Systems	• Tolls, Traffic mgmt., Navigation	

IoT Application Areas and Devices (Cont'd)

Service Sectors	Application Groups	Locations	Devices
Industrial	• Resource Automation	• Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	• Fluid/Processes	• Petro-Chem, Hydro, Carbons, Food, Beverage	
	• Converting/Discrete	• Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	• Distribution	• Pipelines, Conveyance	
Retail	• Specialty	• Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	• Hospitality	• Hotels Restaurants, Bars, Cafes, Clubs	
	• Stores	• Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	• Surveillance	• Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	• Equipment	• Weapons, Vehicles, Ships, Aircraft, Gear	
	• Tracking	• Human, Animal, Postal, Food, Health, Baggage	
	• Public Infrastructure	• Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	• Emergency Services	• Ambulance, Police, Fire, Homeland Security	
IT and Networks	• Public	• Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	• Private Enterprise	• IT/Data Center Office, Privacy Nets	

Module Flow

1

Understand IoT Concepts

2

Discuss IoT Threats and Attacks

3

Discuss IoT Attack Countermeasures

Challenges of IoT

Lack of security and privacy	1	5	Clear text protocols and unnecessary open ports
Vulnerable web interfaces	2	6	Coding errors (buffer overflow)
Legal, regulatory, and rights issues	3	7	Storage issues
Default, weak, and hardcoded credentials	4	8	Difficult to update firmware and OS

IoT Security Problems

APPLICATION



Validation of the inputted string, AuthN, AuthZ, no automatic security updates, default passwords

NETWORK



Firewall, improper communications encryption, services, lack of automatic updates

MOBILE



Insecure API, lack of communication channels encryption, authentication, lack of storage security

CLOUD



Improper authentication, no encryption for storage and communications, insecure web interface

IoT



Application + Network + Mobile + Cloud = IoT

<https://www.hhs.gov>

OWASP Top 10 IoT Threats

01

Weak, Guessable, or
Hardcoded Passwords

02

Insecure Network Services

03

Insecure Ecosystem
Interfaces

04

Lack of Secure Update
Mechanisms

05

Use of Insecure or
Outdated Components

Insufficient Privacy
Protection

06

Insecure Data Transfer
and Storage

07

Lack of Device
Management

08

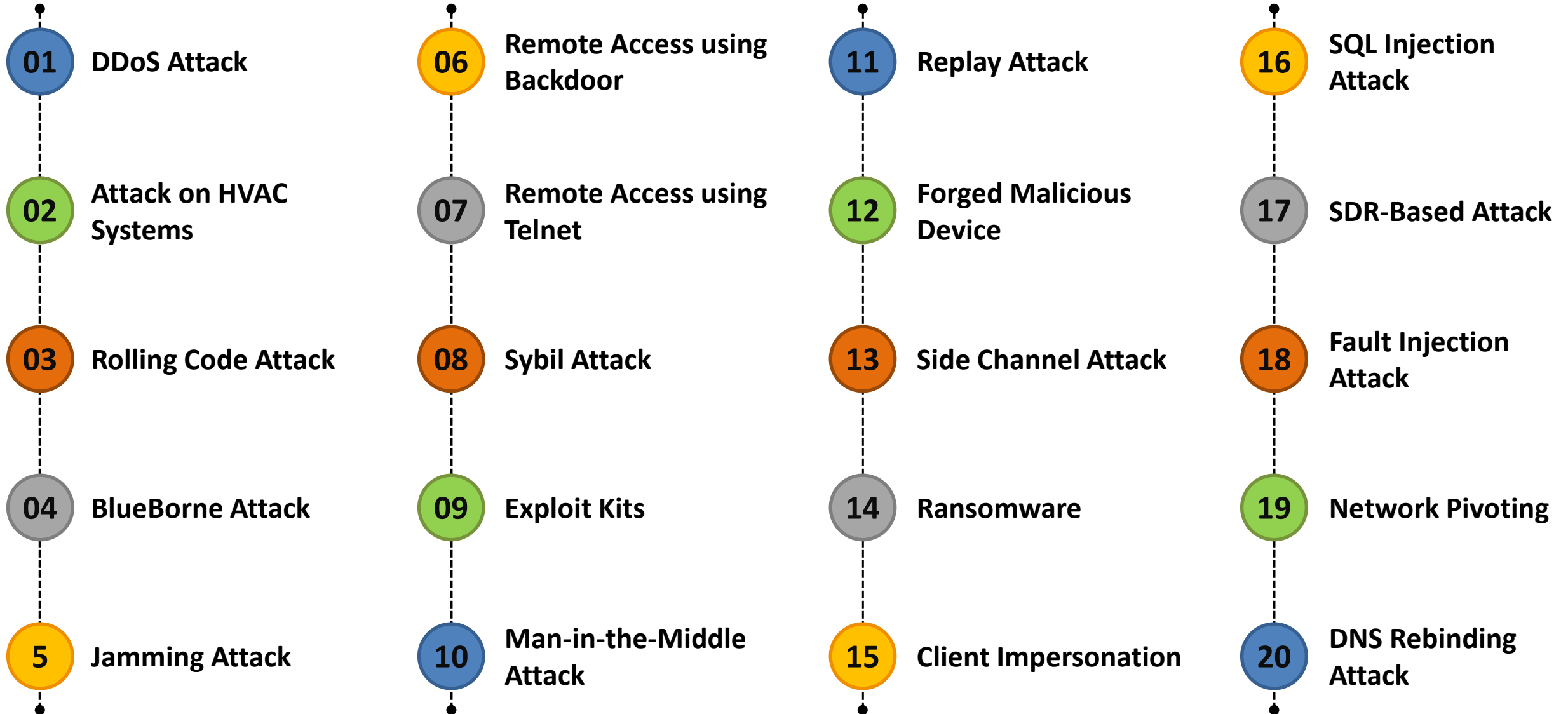
Insecure Default
Settings

09

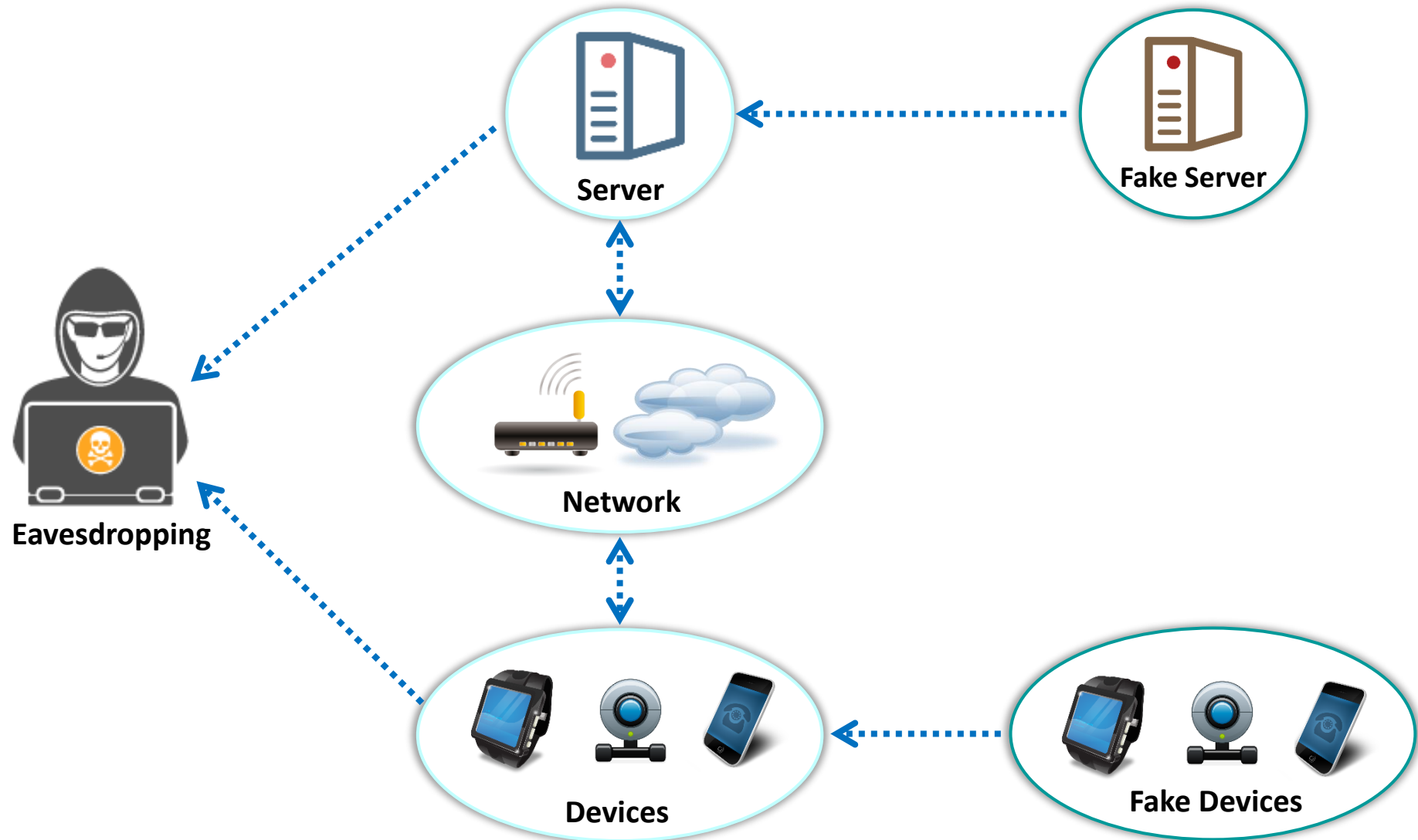
Lack of Physical
Hardening

10

IoT Threats

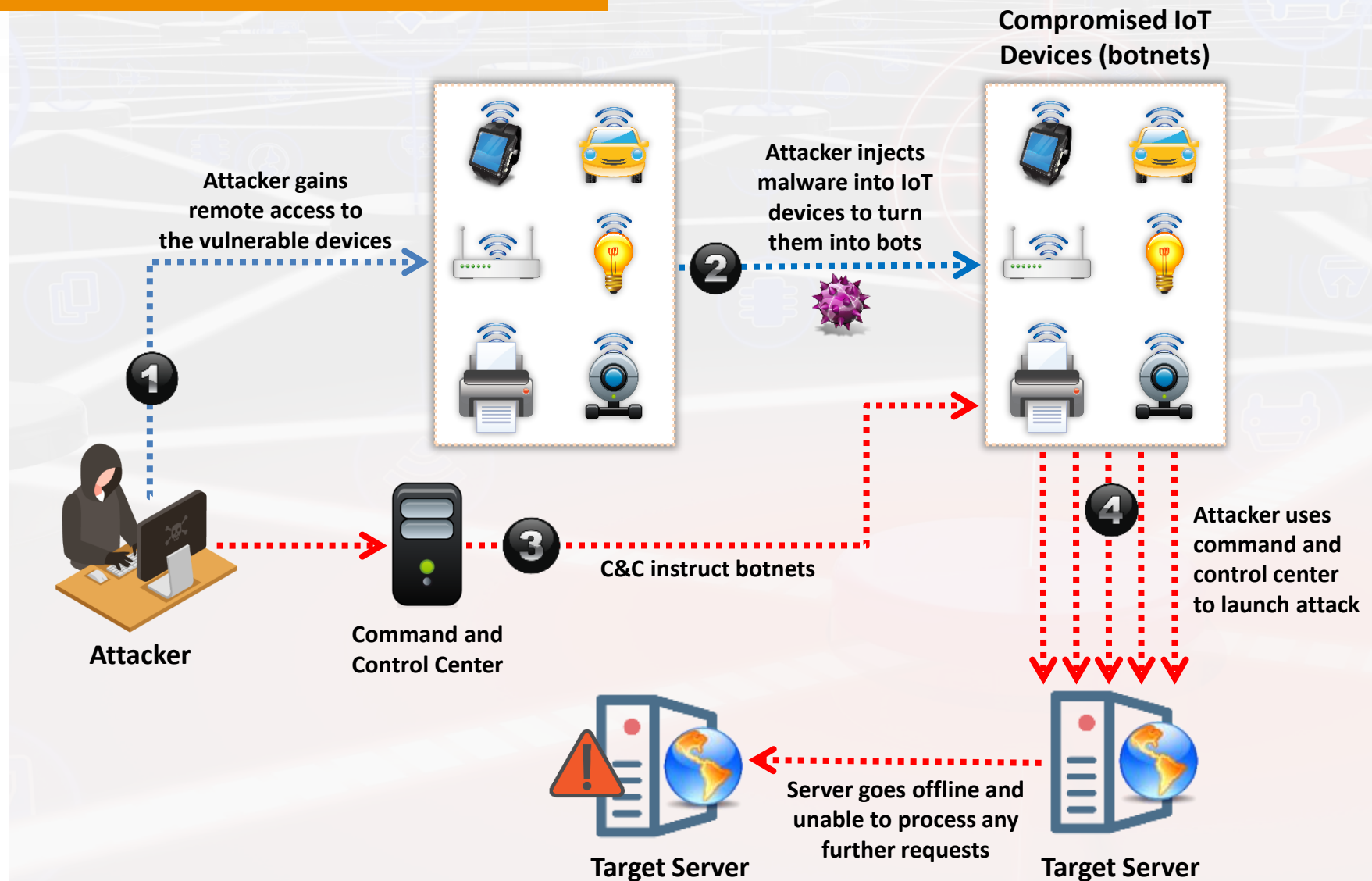


Hacking IoT Devices: General Scenario



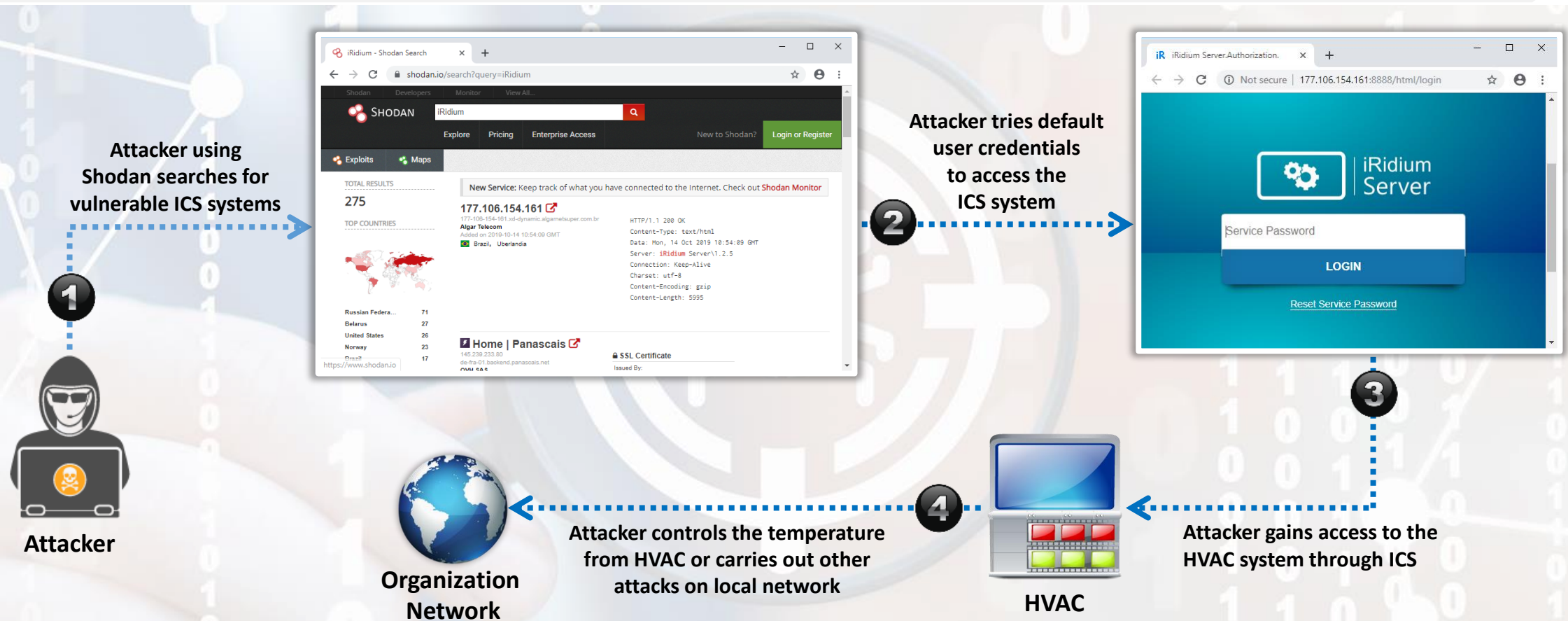
DDoS Attack

- ❑ Attacker initiates the attack by **exploiting the vulnerabilities** in the devices and installing a **malicious software** in their operating systems
- ❑ Multiple infected IoT devices are referred to as an **Army of Botnets**
- ❑ The target is attacked with a **large volume of requests** from multiple IoT devices present in different locations

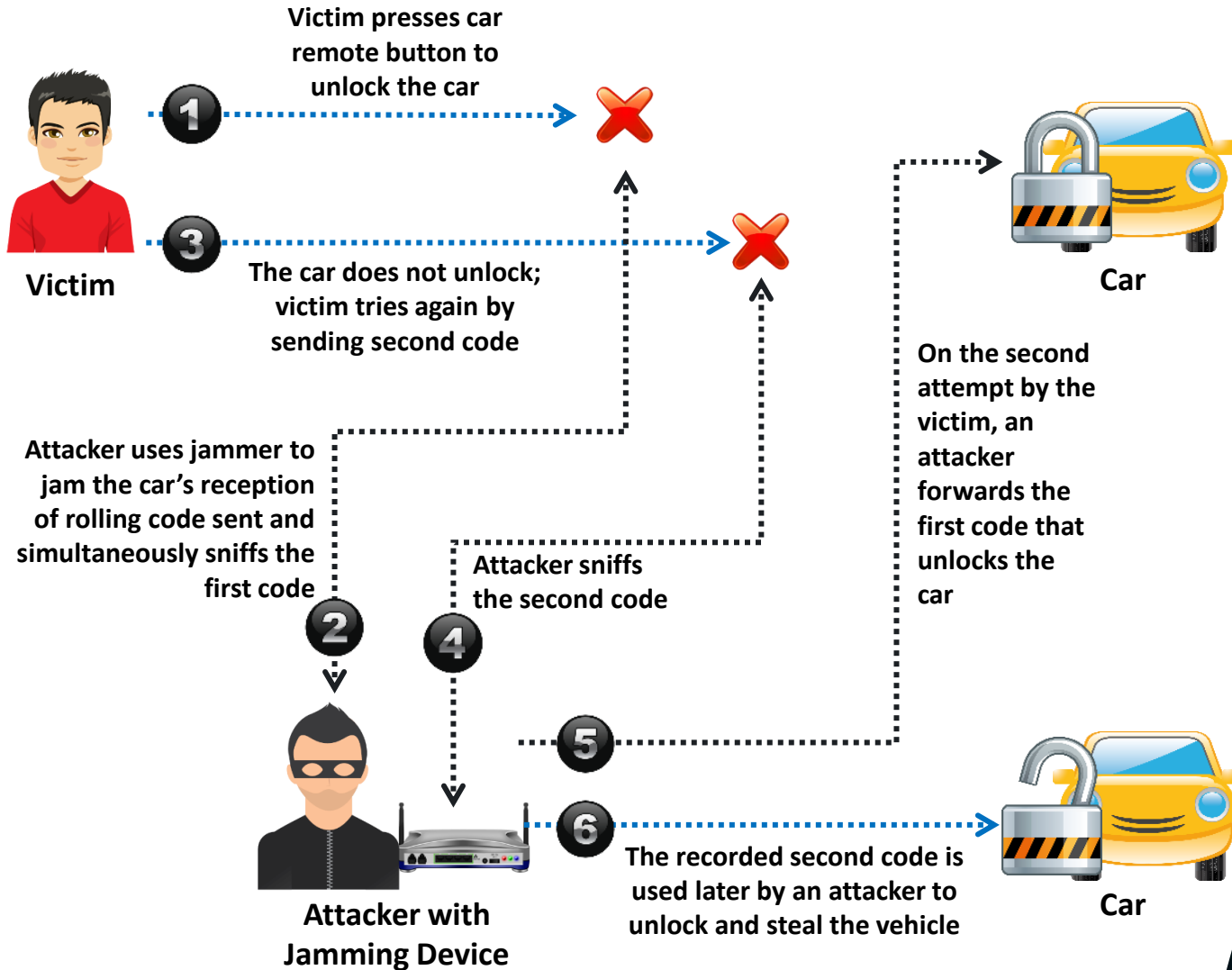


Exploit HVAC

- ❑ Many organizations use Internet-connected heating, ventilation, and air conditioning (HVAC) systems without implementing security mechanisms; this gives attackers a gateway to **hack corporate systems**
- ❑ HVAC systems have many **security vulnerabilities** that are exploited by attackers to steal login credentials, gain access to the HVAC system, and perform further attack on the organization's network



Rolling Code Attack



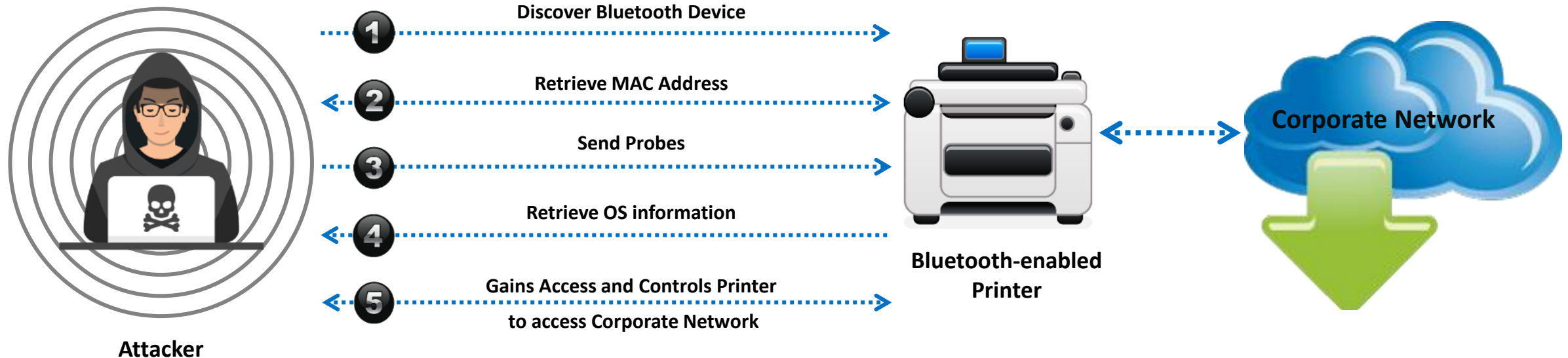
BlueBorne Attack



A BlueBorne attack is performed on **Bluetooth connections to gain access** and take full control of the target device



After gaining access to a device, the attacker can penetrate any corporate network using that device to **steal critical information** about the organization and **spread malware** to nearby devices

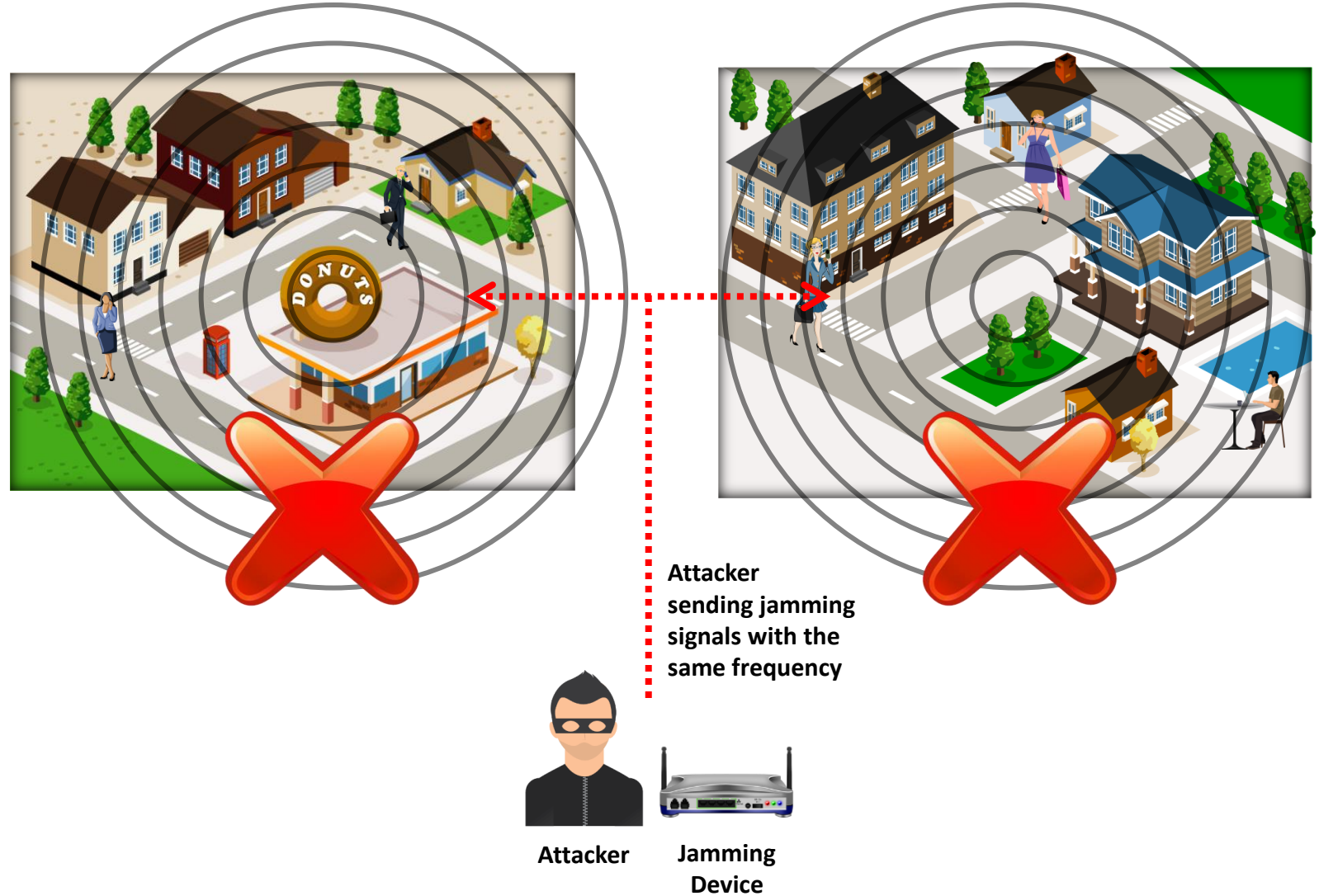


Jamming Attack

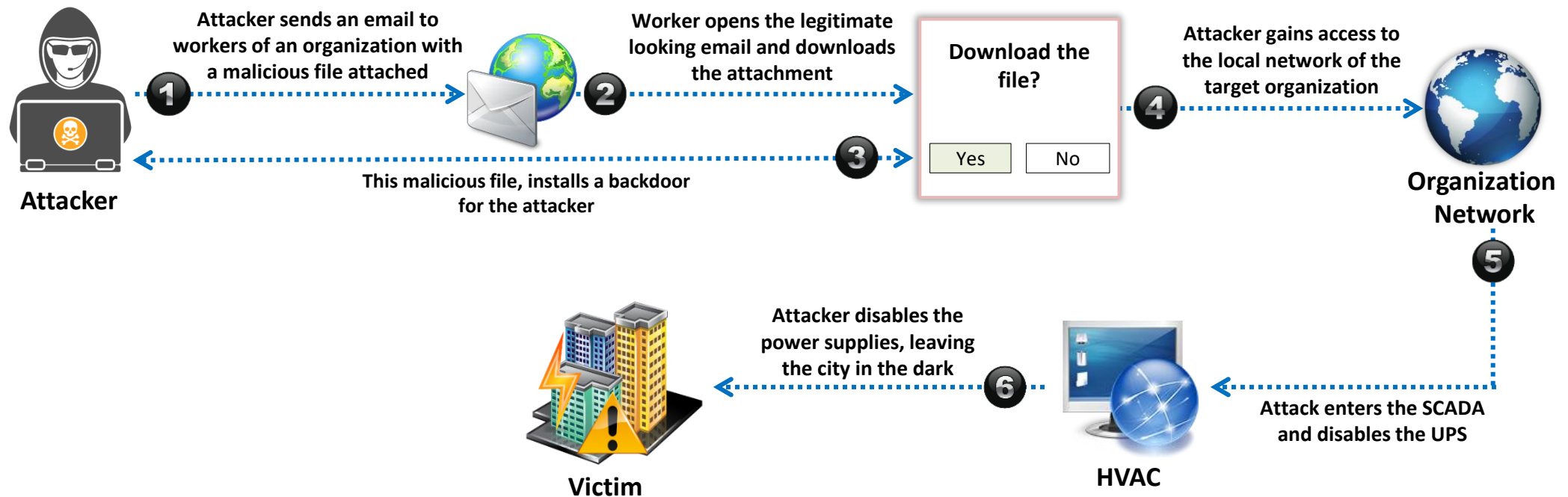
Jamming is a type of attack in which the **communications between wireless IoT devices are jammed** so that they can be compromised

An attacker transmits **radio signals randomly** with the same frequency as the sensor nodes for communication

As a result, the network gets jammed, which **disables the endpoints from sending or receiving** any messages



Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor



SDR-Based Attacks on IoT



The attacker uses software defined radio (SDR) to **examine the communication signals in the IoT network** and **sends spam content** or texts to the interconnected devices



+ **Replay Attack**

- The attacker obtains the **specific frequency** used for sharing information between connected devices and captures the original data when a command is initiated by these devices
- The attacker segregates the command sequence and injects it into the IoT network



+ **Cryptanalysis Attack**

- The attacker uses the same procedure as that followed in a replay attack, along with reverse engineering of the protocol to capture the **original signal**
- The attacker must be skilled in cryptography, communication theory, and modulation schemes to perform this attack



+ **Reconnaissance Attack**

- The attacker obtains information about the target device from the device's specifications
- The attacker then uses a multimeter to **investigate the chipset** and mark some identifications such as ground pins to discover the product ID and other information

Fault Injection Attacks

- ❑ Fault injection attacks, also known as **Perturbation attacks**, occur when a perpetrator injects any faulty or malicious program into the system to compromise the system security

Types of Fault Injection Attacks



Optical, Electro Magnetic Fault Injection (EMFI), Body Bias Injection (BBI)

Attackers inject faults into the device by using projecting lasers and electromagnetic pulses



Frequency/Voltage Tampering

Attackers tamper with the operating conditions, modify the level of the power supply and/or alter the clock frequency of the chip



Power/Clock/Reset Glitching

Attackers inject faults or glitches into the power supply and clock network of the chip



Temperature Attacks

Attackers alter the temperature for operating the chip, affecting the whole operating environment

Capturing and Analyzing IoT Traffic using Wireshark

01

Run Nmap to identify IoT devices using insecure HTTP ports

```
nmap -p 80,81,8080,8081 <Target IP address range>
```

02

Run **ifconfig** to identify your wireless card, here **wlan0**

03

Run **Airmon-ng** to put the wireless card in monitor mode
airmon-ng start wlan0

04

Run **Airodump-ng** to scan all the nearby wireless networks
airodump-ng start wlan0mon

05

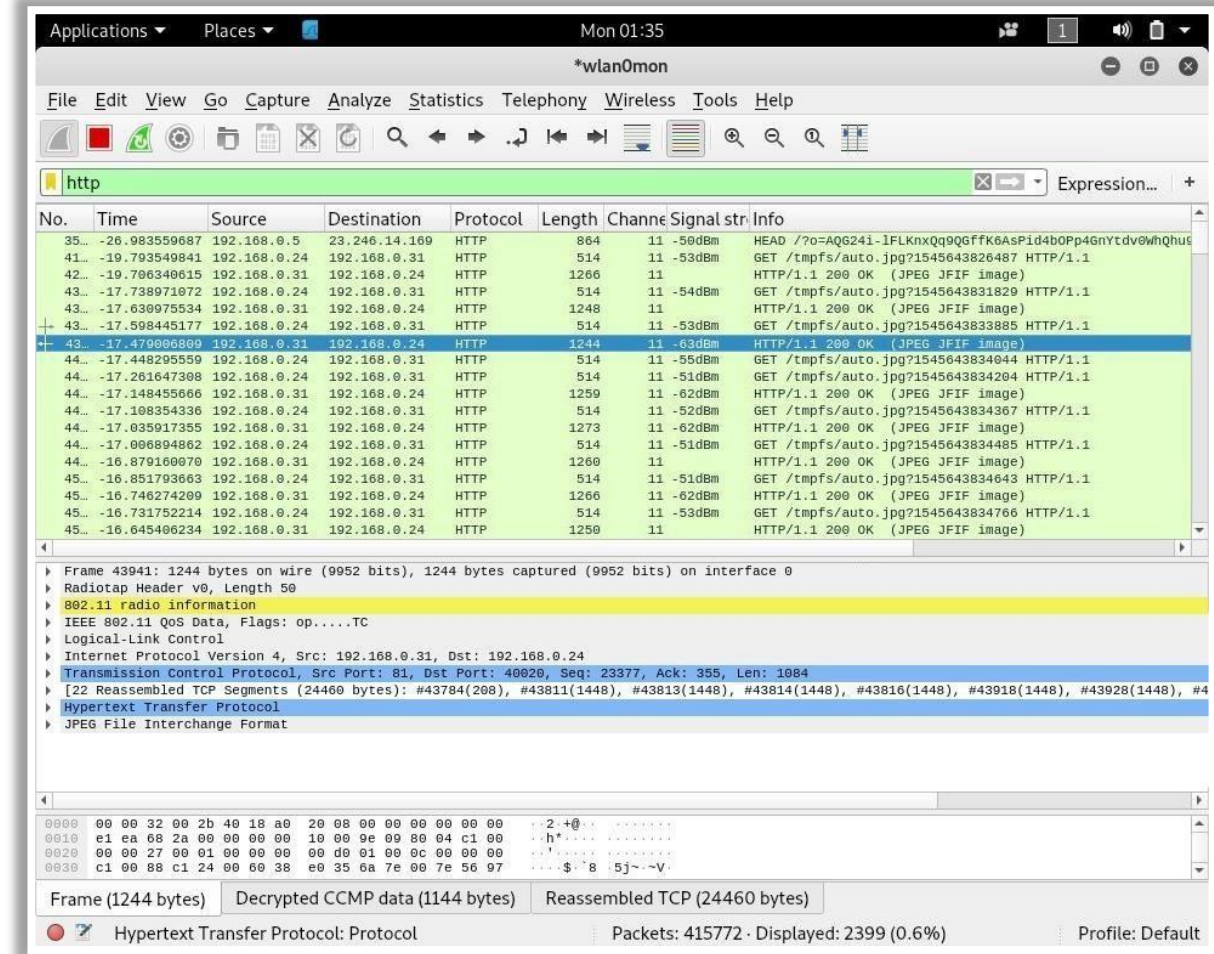
Discover the target wireless network and note down the corresponding channel to sniff the traffic using Wireshark

06

Next, setup your wireless card to listen to the traffic on the same channel using **Airmon-ng**
airmon-ng start wlan0mon 11

07

Launch Wireshark and double-click the interface that was kept in monitor mode, here **wlan0mon** and start capturing the traffic

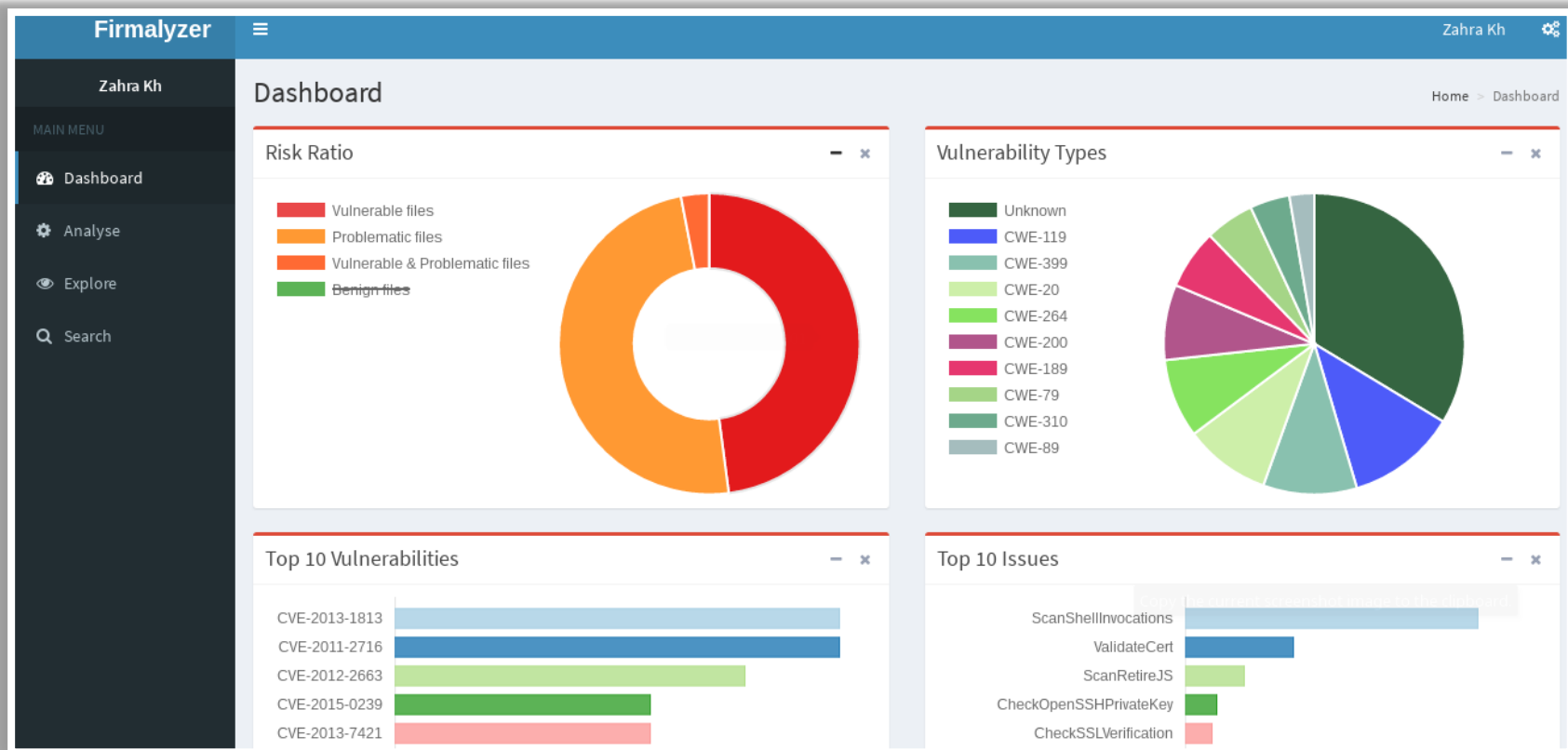


IoT Attack Tools

Firmalyzer



Firmalyzer enables device vendors and security professionals to perform an **automated security assessment** on software that powers IoT devices (firmware) to **identify configuration** and **application vulnerabilities**



<https://firmalyzer.com>



RIoT Vulnerability Scanner
<https://www.beyondtrust.com>



Foren6
<https://cetic.github.io>



IoT Inspector
<https://www.iot-inspector.com>



RFCrack
<https://github.com>



HackRF One
<https://greatscottgadgets.com>

Module Flow

A hand is shown interacting with a tablet. The tablet screen displays a grid of hexagonal icons representing various IoT concepts like a lightbulb, a person, a gear, and a document. Overlaid on the screen is a semi-transparent layer of code snippets, including `onPageChangeListener`, `onPageSelected`, and `onPageScrollStateChanged`. The background is a blurred image of a person's face.

1

Understand IoT Concepts

2

Discuss IoT Threats and Attacks

3

Discuss IoT Attack Countermeasures

IoT Attack Countermeasures



Disable the “**guest**” and “**demo**” user accounts if enabled



Use the “**Lock Out**” feature to lock out accounts for excessive invalid login attempts



Implement **strong authentication** mechanisms



Locate control system networks and devices behind firewalls and isolate them from the business network



Implement **end-to-end encryption** and use Public Key Infrastructure (PKI)



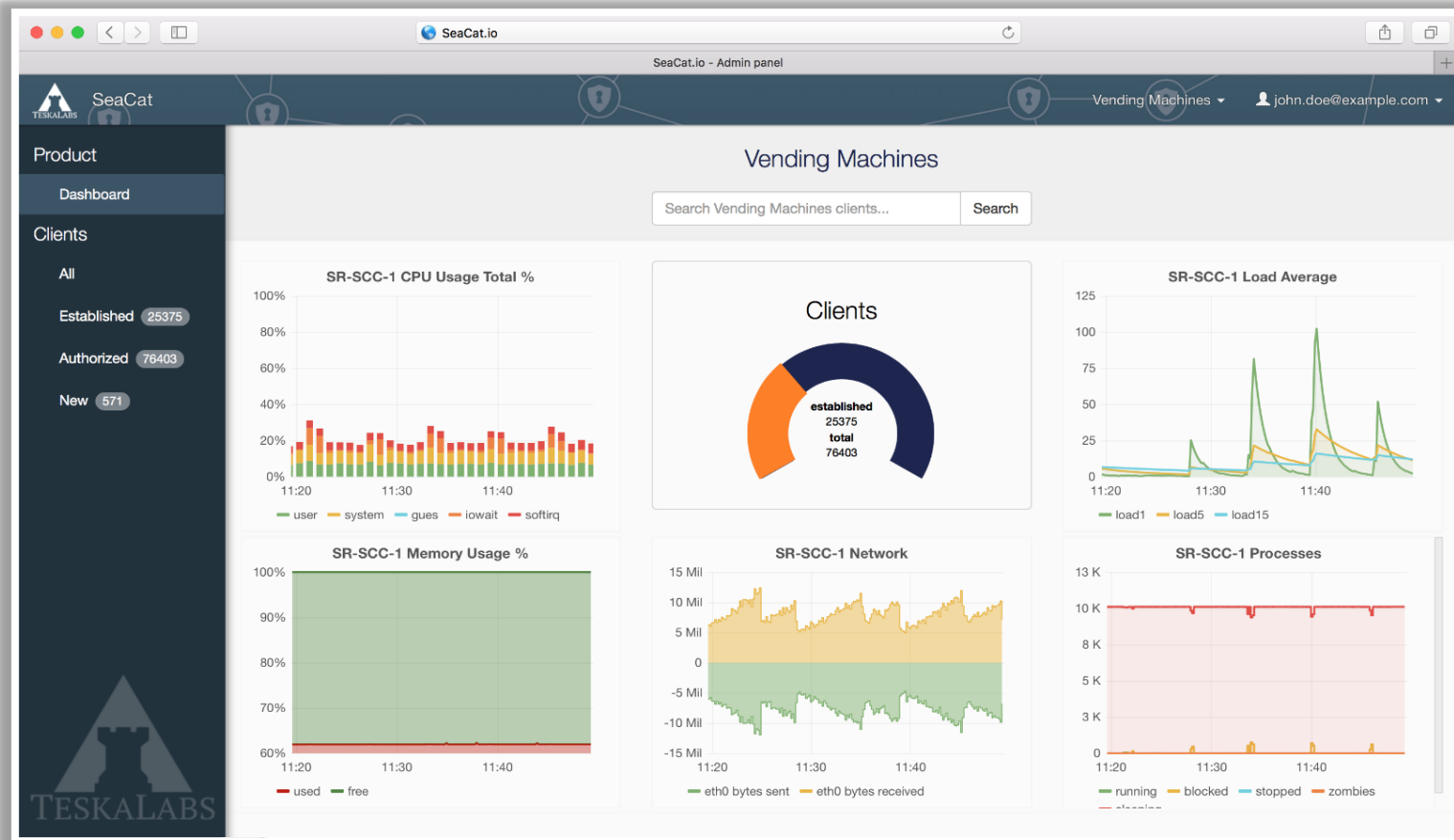
Patch vulnerabilities and **update the device firmware** regularly



IoT Security Tools

SeaCat.io

SeaCat.io is a **security-first SaaS technology** to operate IoT products in a reliable, scalable, and secure manner



<https://www.teskalabs.com>



DigiCert IoT Device Manager
<https://www.digicert.com>



FortiNAC
<https://www.fortinet.com>



darktrace
<https://www.darktrace.com>



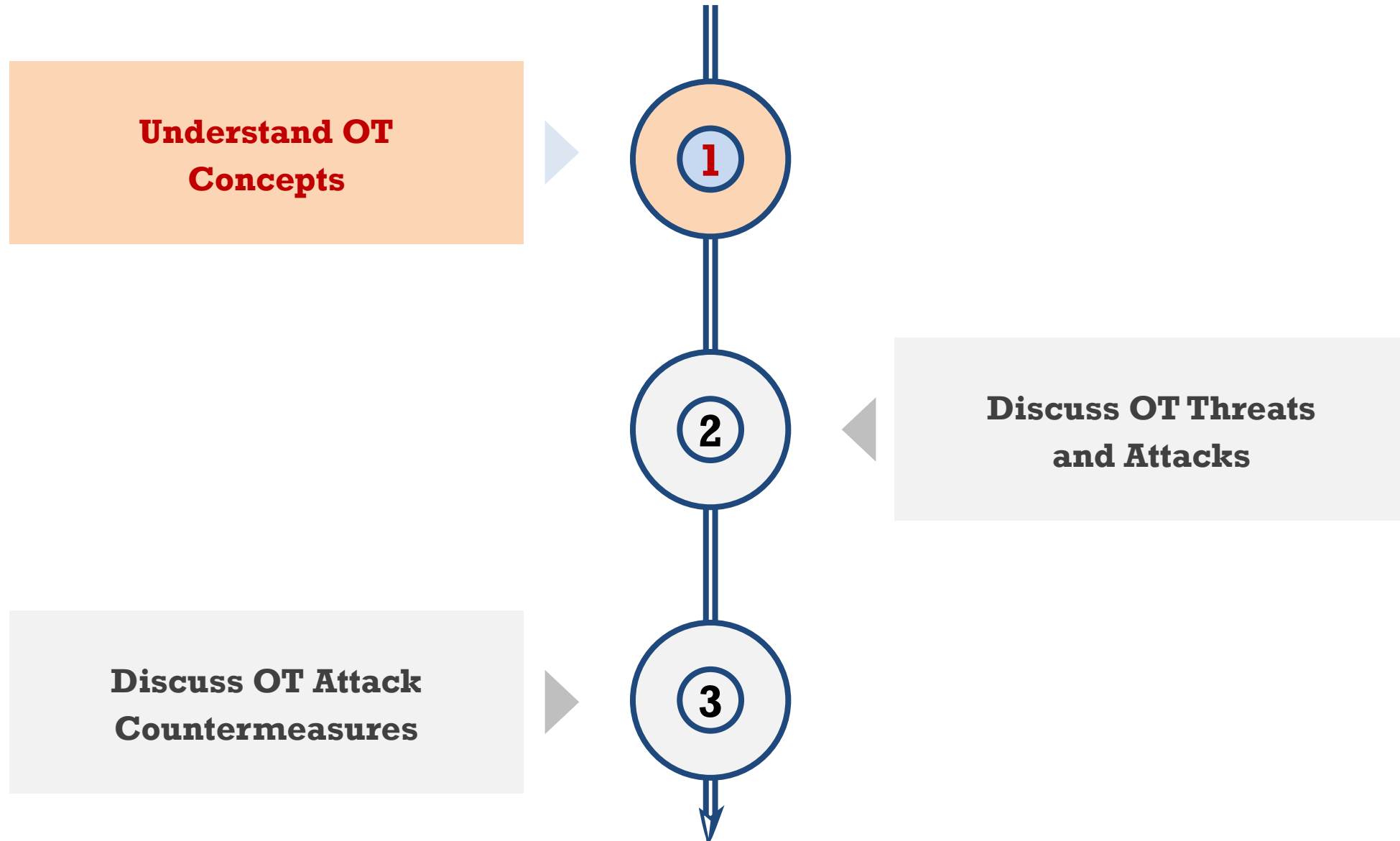
Symantec Critical System Protection
<https://www.symantec.com>



Cisco IoT Threat Defense
<https://www.cisco.com>

OT Attacks

Module Flow



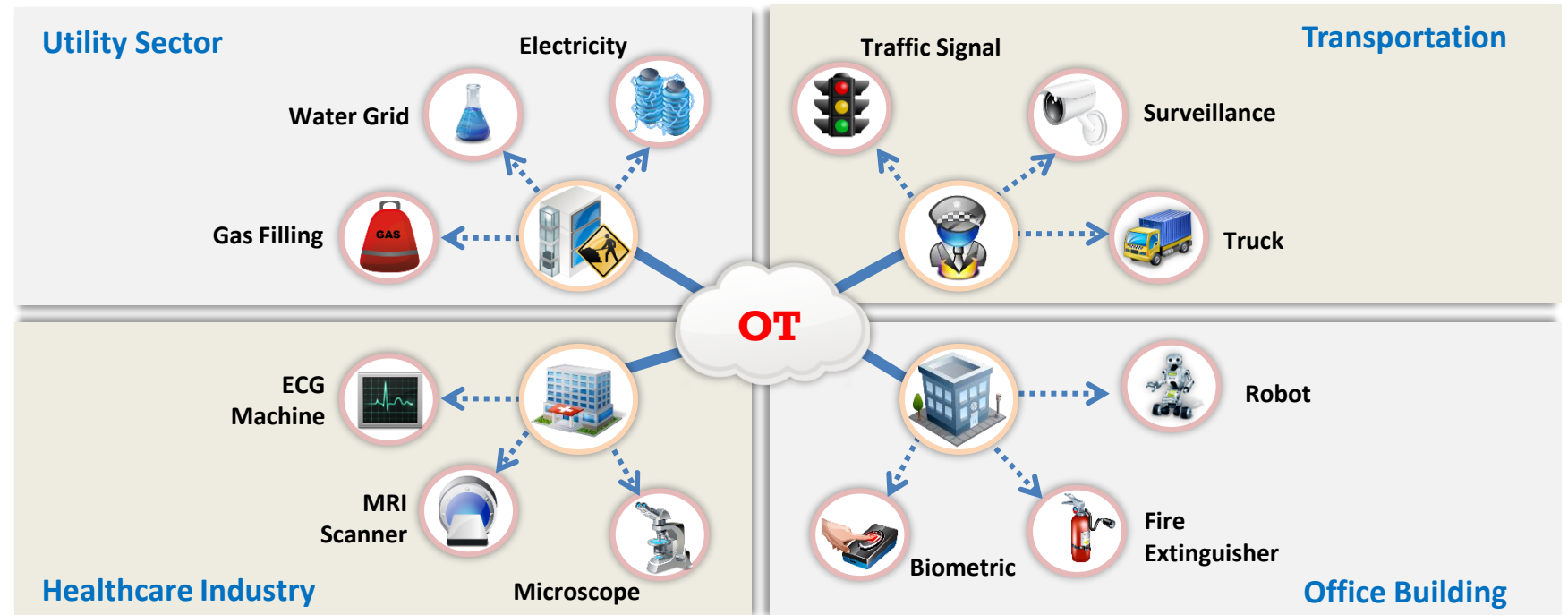
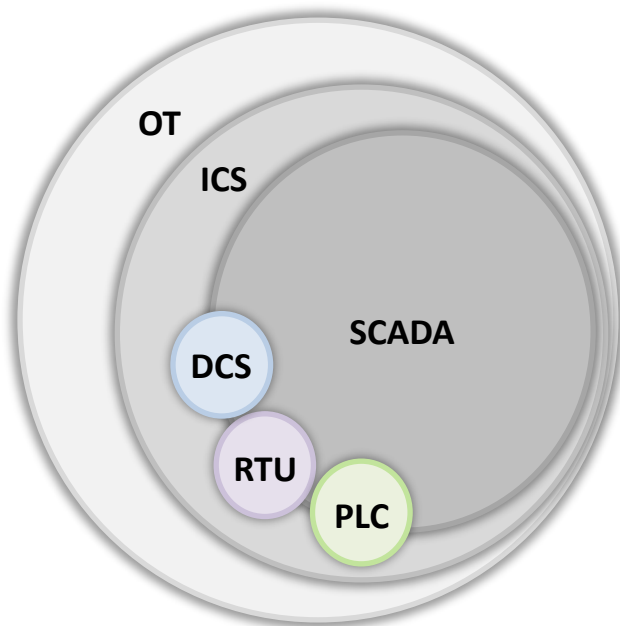
What is OT?



Operational Technology (OT) is the software and hardware designed to **detect or cause changes in industrial operations** through direct monitoring and/or controlling of industrial physical devices



OT consists of **Industrial Control Systems** (ICS) to monitor and control the industrial operations



Essential Terminology



Assets

OT systems consist of **physical assets** such as sensors and actuators, servers, workstations, network devices, and PLCs, and logical assets such as flow graphics, program logic, databases, firmware, and firewall rules.



Zones and Conduits

A **network segregation technique** used to isolate the networks and assets to impose and maintain strong access control mechanisms.



Industrial Network

A network of **automated control systems** is known as an industrial network.



Business Network

It comprises of a network of systems that offer **information infrastructure** to the business.

Essential Terminology (Cont'd)



Industrial Protocols

Protocols used for **serial communication** and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.



Network Perimeter

It is the outermost boundary of a network zone i.e. **closed group of assets**



Electronic Security Perimeter

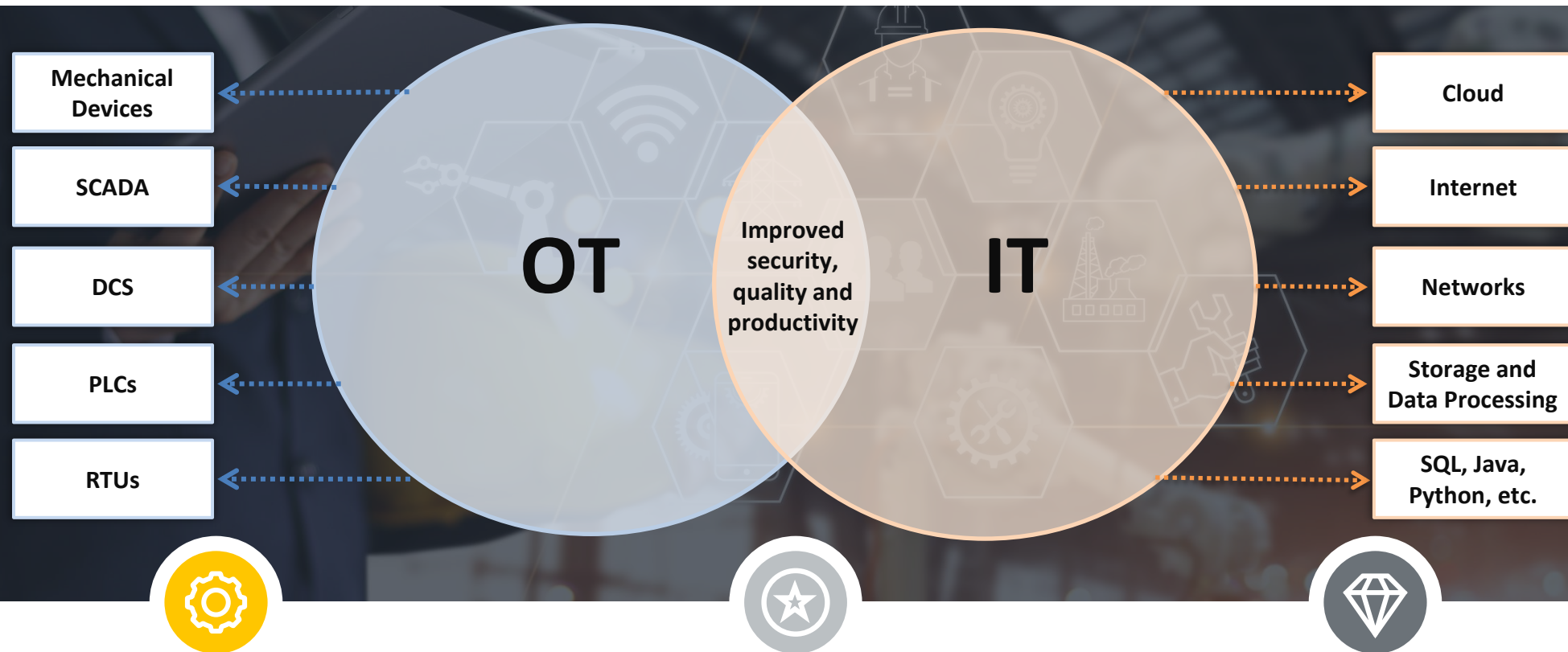
It is referred to as the **boundary** between secure and insecure zones



Critical Infrastructure

A collection of **physical or logical systems** and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health

IT/OT Convergence (IIOT)



IT/OT convergence is the integration of **IT computing systems and OT operation monitoring systems** to bridge the gap between IT/OT technologies for improving overall security, efficiency, and productivity

The IT/OT convergence can enable smart manufacturing known as industry 4.0, where IoT applications are used in industrial operations

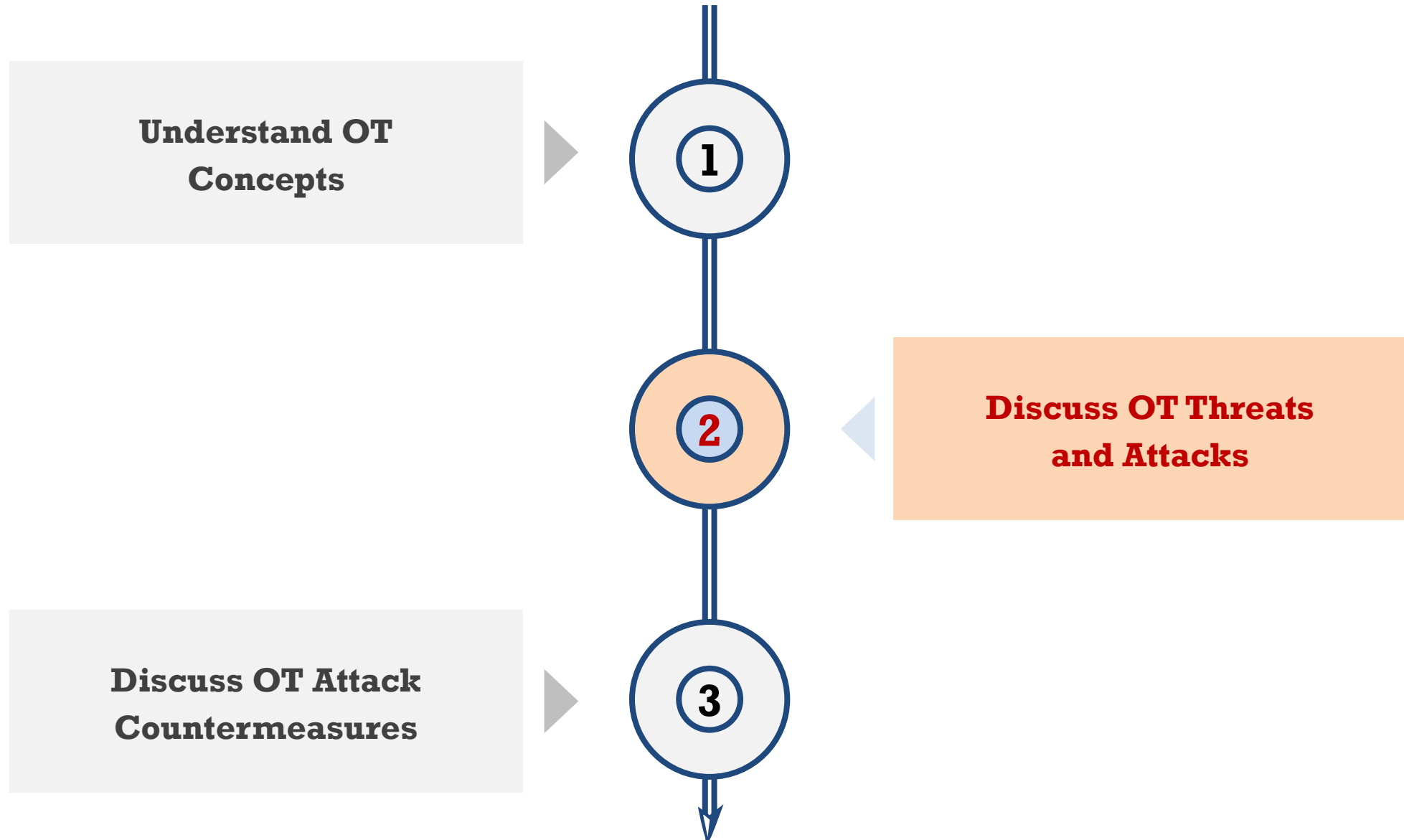
Using this Internet of Things (IoT) for industrial operations such as monitoring supply chains, manufacturing and management systems is referred to as **Industrial Internet of Things (IIoT)**

The Purdue Model

- ❑ The Purdue model is derived from the **Purdue Enterprise Reference Architecture** (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks
- ❑ It consists of three zones

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Module Flow



Challenges of OT

1

Lack of visibility

2

Plain-text passwords

3

Network complexity

4

Legacy technology

5

Lack of anti-virus protection

6

Lack of skilled security professionals

7

Rapid pace of change

8

Outdated systems

9

Haphazard modernization

10

Convergence with IT

11

**Unique production networks /
Proprietary software**

12

Vulnerable communication protocols

OT Threats

01 Maintenance and Administrative Threat

02 Data Leakage

03 Protocol Abuse

04 Potential Destruction of ICS Resources

05 Reconnaissance Attacks

06 Denial-of-Service Attacks



OT Threats Cont'd)

07

HMI-based Attacks

08

**Exploiting Enterprise
Specific Systems and Tools**

09

Spear Phishing

10

Malware Attacks

11

**Exploiting Unpatched
Vulnerabilities**

12

Side-Channel Attacks

13

**Buffer Overflow
Attacks**

14

**Exploiting RF Remote
Controllers**

HMI-based Attacks



Attackers often try to compromise the HMI system as it is the core hub that **controls the critical infrastructure**



Attackers gain access to the HMI systems to cause **physical damage to the SCADA devices** or collect sensitive information related to the critical architecture

SCADA vulnerabilities exploited by attackers to perform HMI-based attacks:

Memory Corruption

01



03

Credential Management



Lack of Authorization/Authentication
and Insecure Defaults

02



04

Code Injection



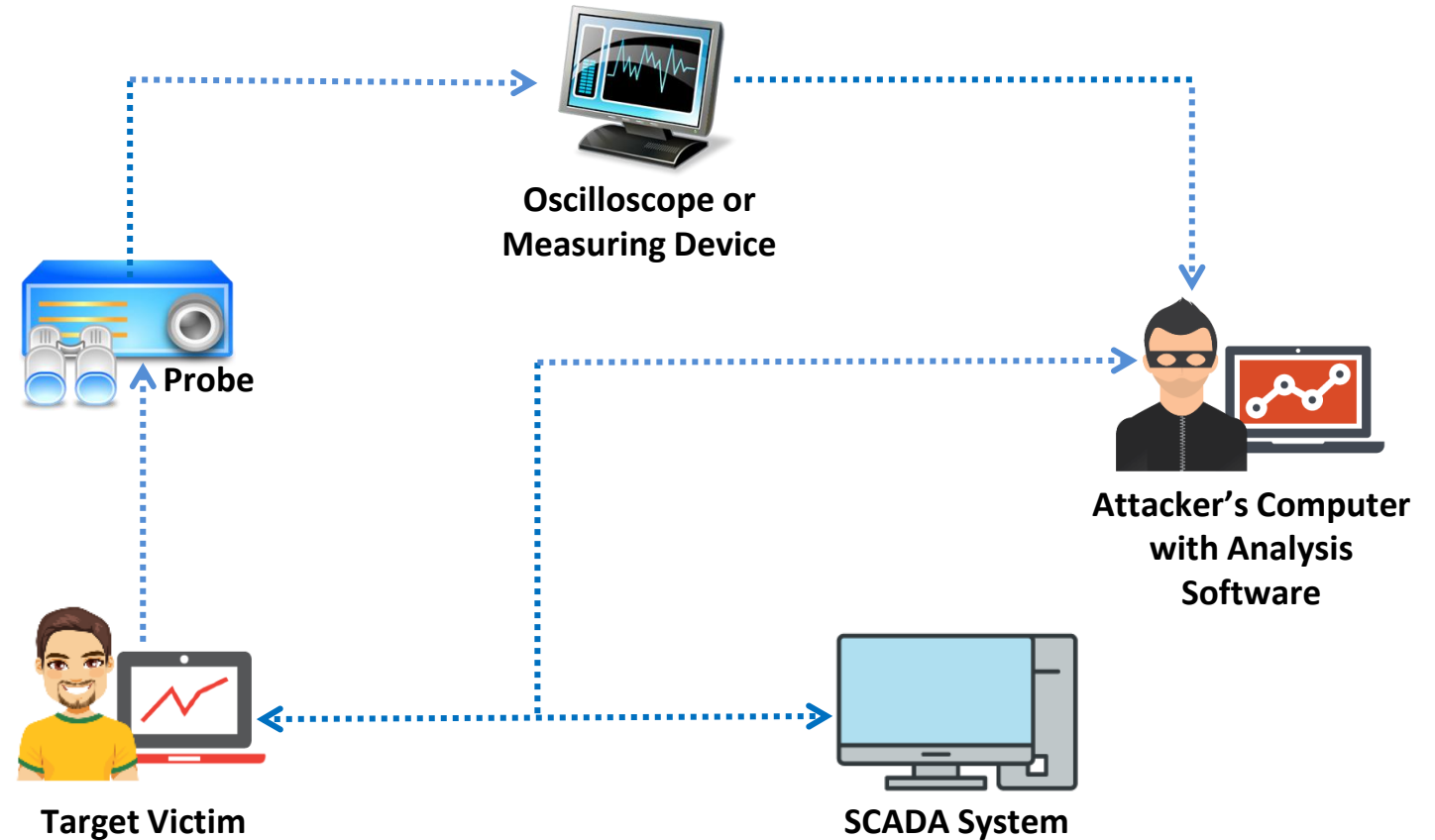
Side-Channel Attacks



Attackers perform a side-channel attack by monitoring its **physical implementation** to obtain critical information from a target system



Attackers use two techniques namely **timing analysis and power analysis** to perform side-channel attacks on the target OT systems



Side-Channel Attacks (Cont'd)



Timing Analysis

- ❑ Attackers monitor the amount of time the device is taking to **finish one complete** password authentication process to determine the number of correct characters



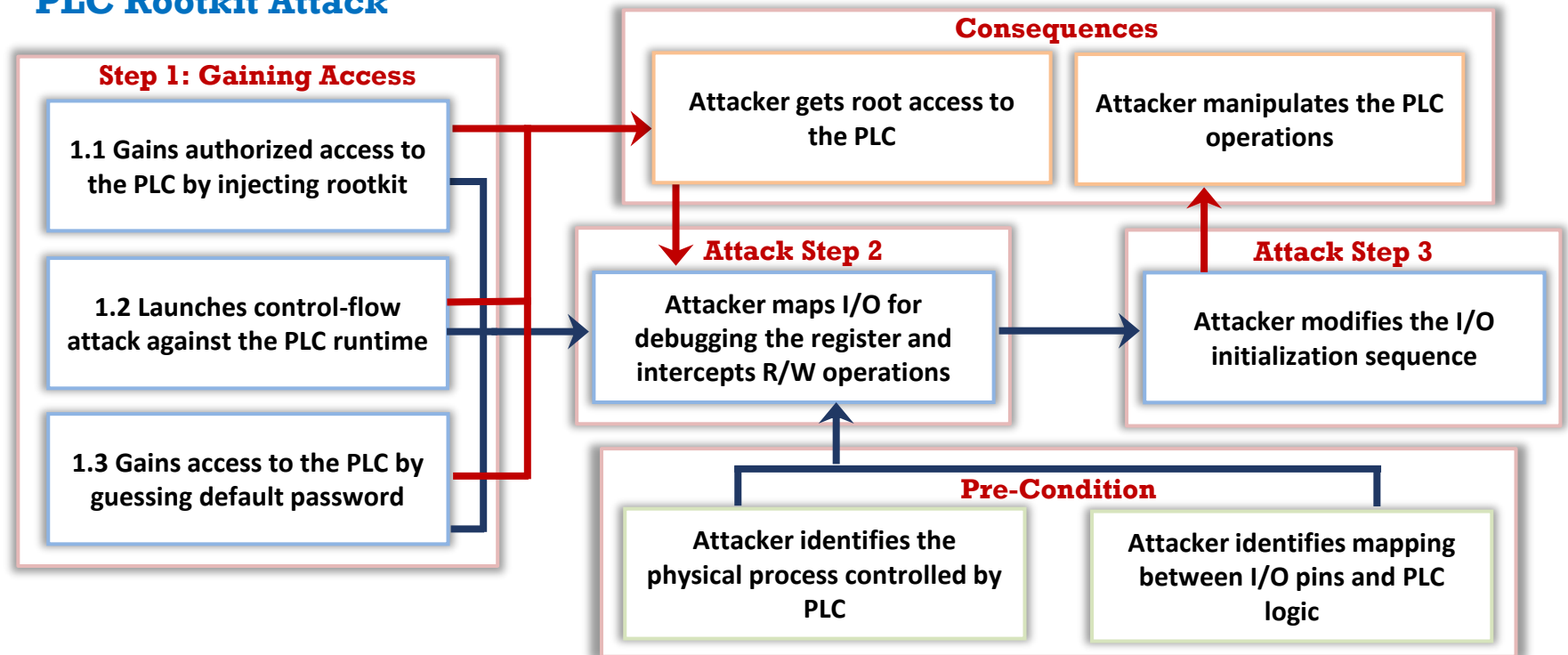
Power Analysis

- ❑ Attackers observe the change in **power consumption** of semiconductors during clock cycles
- ❑ By observing the **power profile**, one character of the password can be retrieved comparing the correct character with the wrong character

Hacking Programmable Logic Controller (PLC)

- ❑ Programmable Logic Controllers (PLCs) are susceptible to cyber-attacks as they are used for **controlling the physical processes** of critical infrastructure
- ❑ Attackers identify PLCs exposed to the Internet using online tools such as **Shodan**
- ❑ Attackers can tamper with the integrity and availability of PLC systems by exploiting **pin control operations**

PLC Rootkit Attack

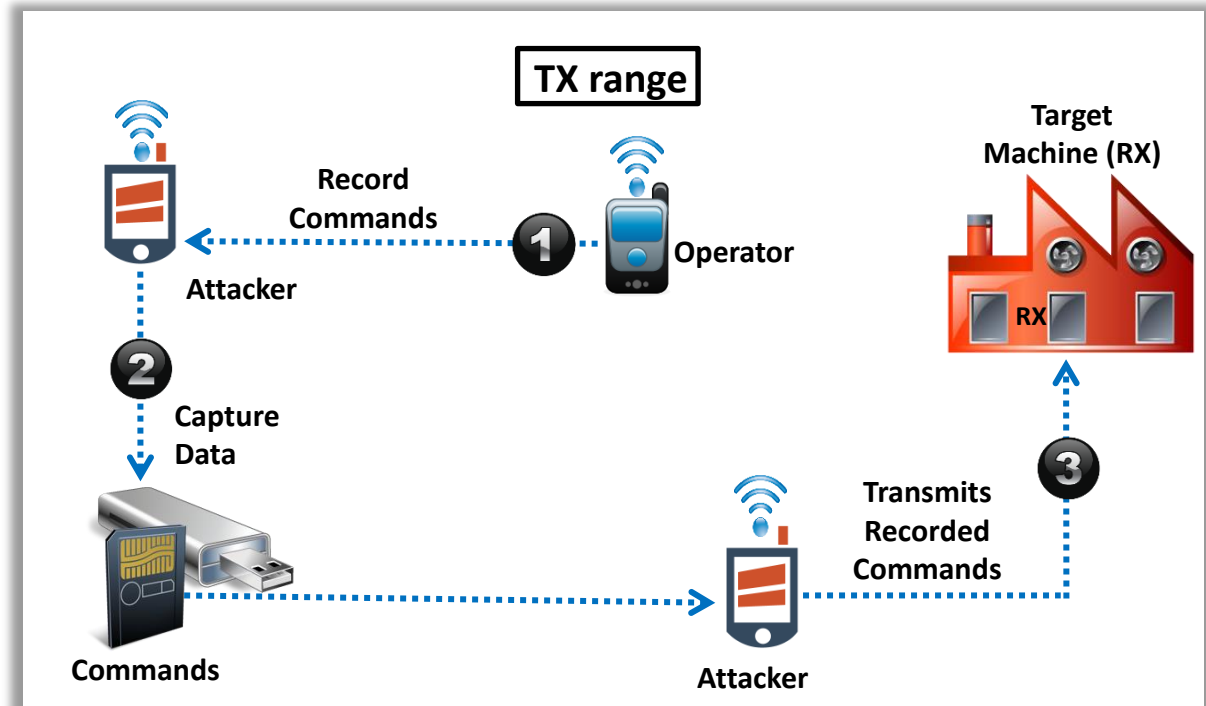


Hacking Industrial Systems through RF Remote Controllers

- ❑ Most industrial machines are **operated via remote controllers** that are used in various industries such as manufacturing, logistics, mining, and constructions for automation or to control machines
- ❑ Improper security implementations in the devices operating via remote controllers can **pose severe risks** to the industrial systems

Replay Attack

Attackers **record the commands** transmitted by an operator and replay them to the target system to gain basic control over the system

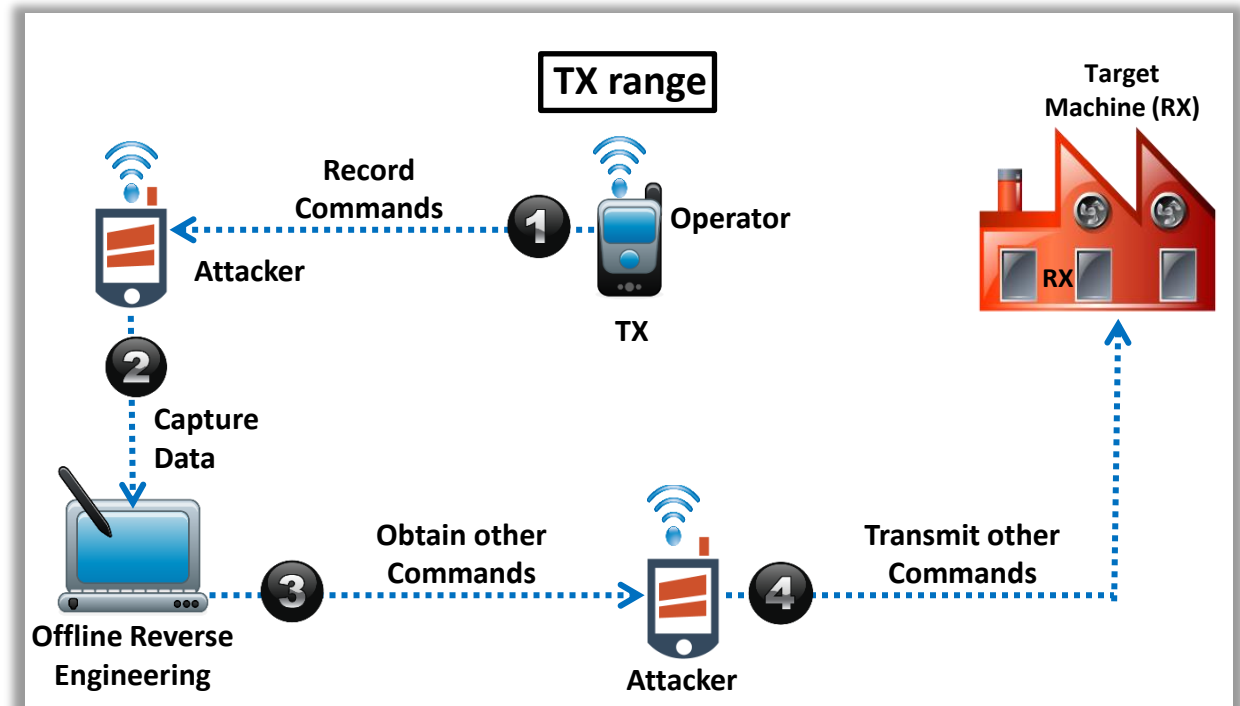


Hacking Industrial Systems through RF Remote Controllers (Cont'd)

Command Injection



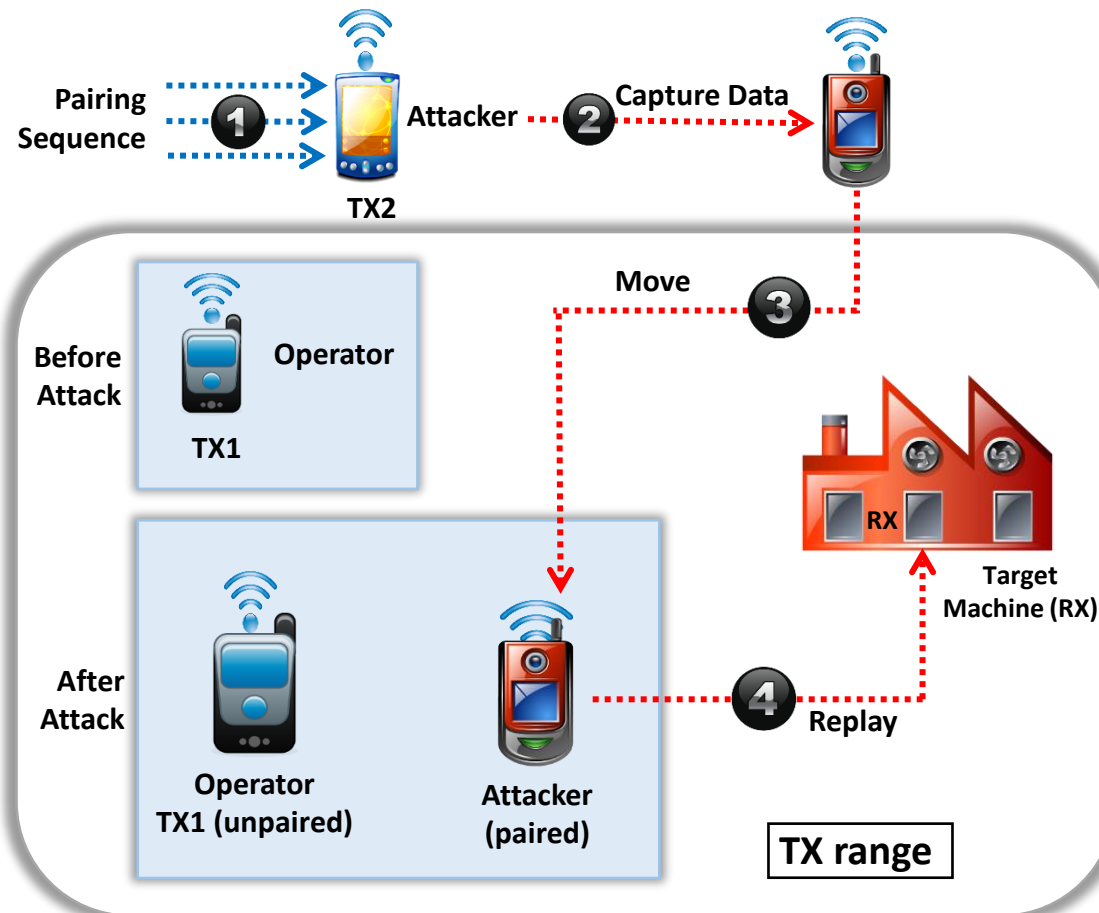
Attackers **alter RF packets** or inject their own packets employing reverse engineering techniques to gain complete access over the target machine



Hacking Industrial Systems through RF Remote Controllers (Cont'd)

Re-pairing with Malicious RF controller

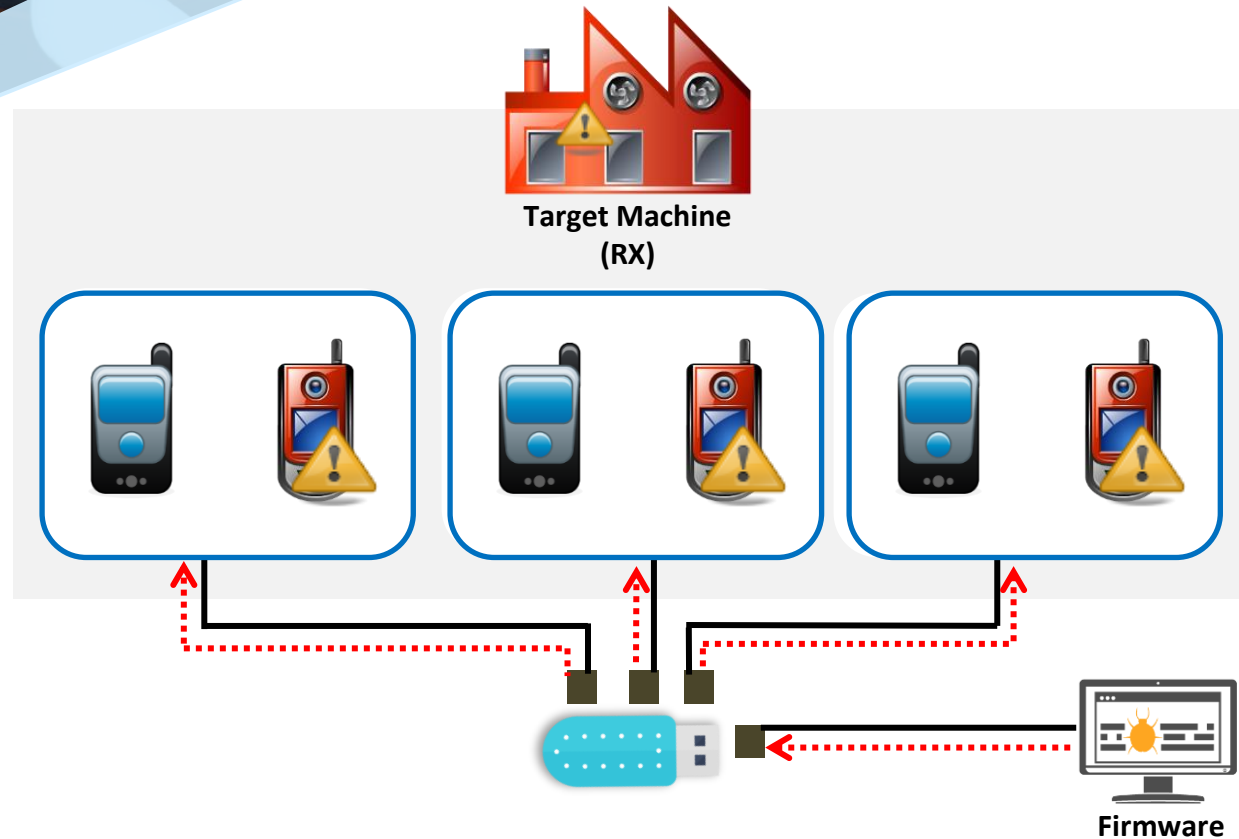
- ❑ Attackers hijack the original remote controller and pair it with the machine using a **malicious RF controller**, which they disguise as a legitimate one



Hacking Industrial Systems through RF Remote Controllers (Cont'd)

Malicious Reprogramming Attack

- ❑ Attackers **inject malware** into the firmware of the remote controllers to maintain a persistent and completely remote access to the system

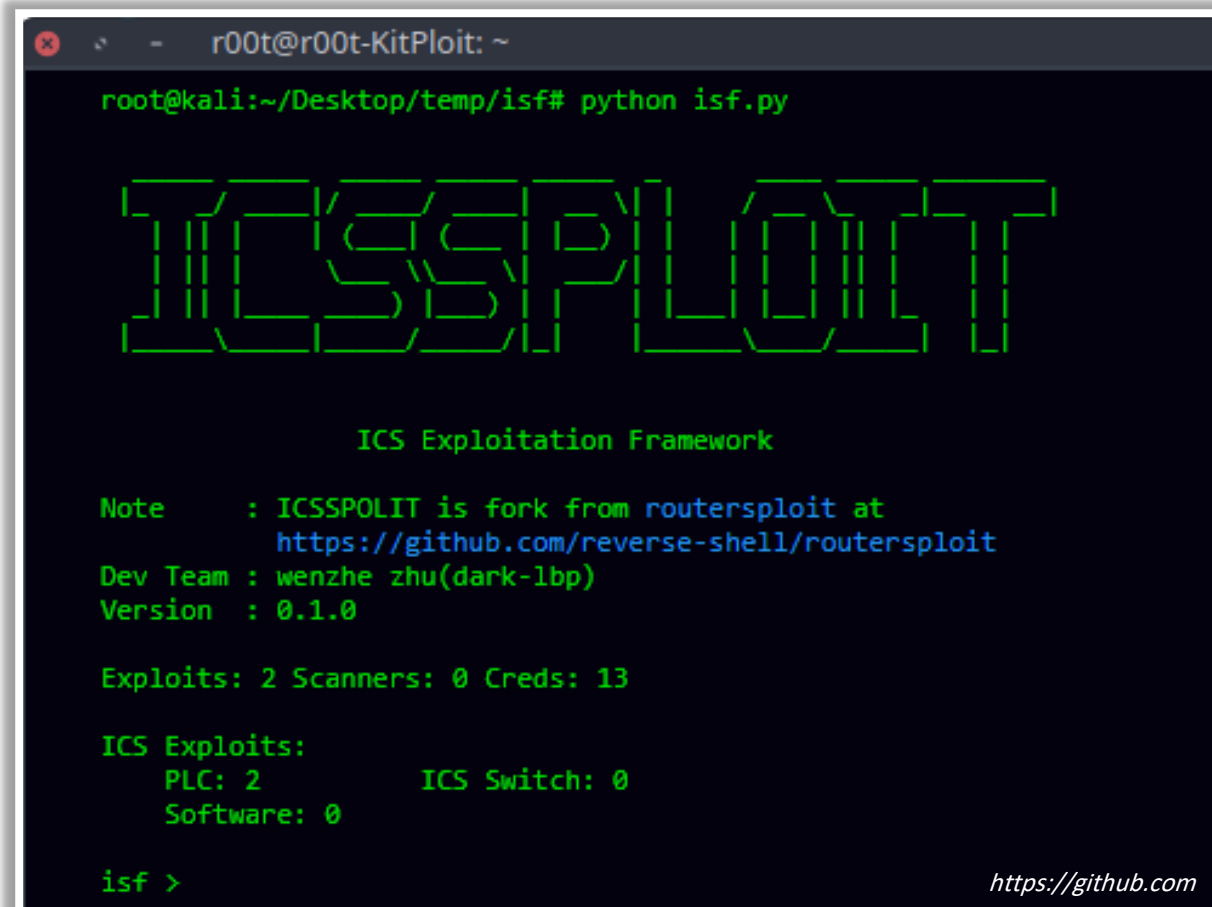


OT Attack Tools



ICS Exploitation Framework (ISF)

ICS Exploitation Framework (ISF) is an **exploitation framework** based on Python and is like the Metasploit framework



SCADA Shutdown Tool

<https://github.com>



GRASSMARLIN
<https://github.com>



Metasploit

<https://www.metasploit.com>

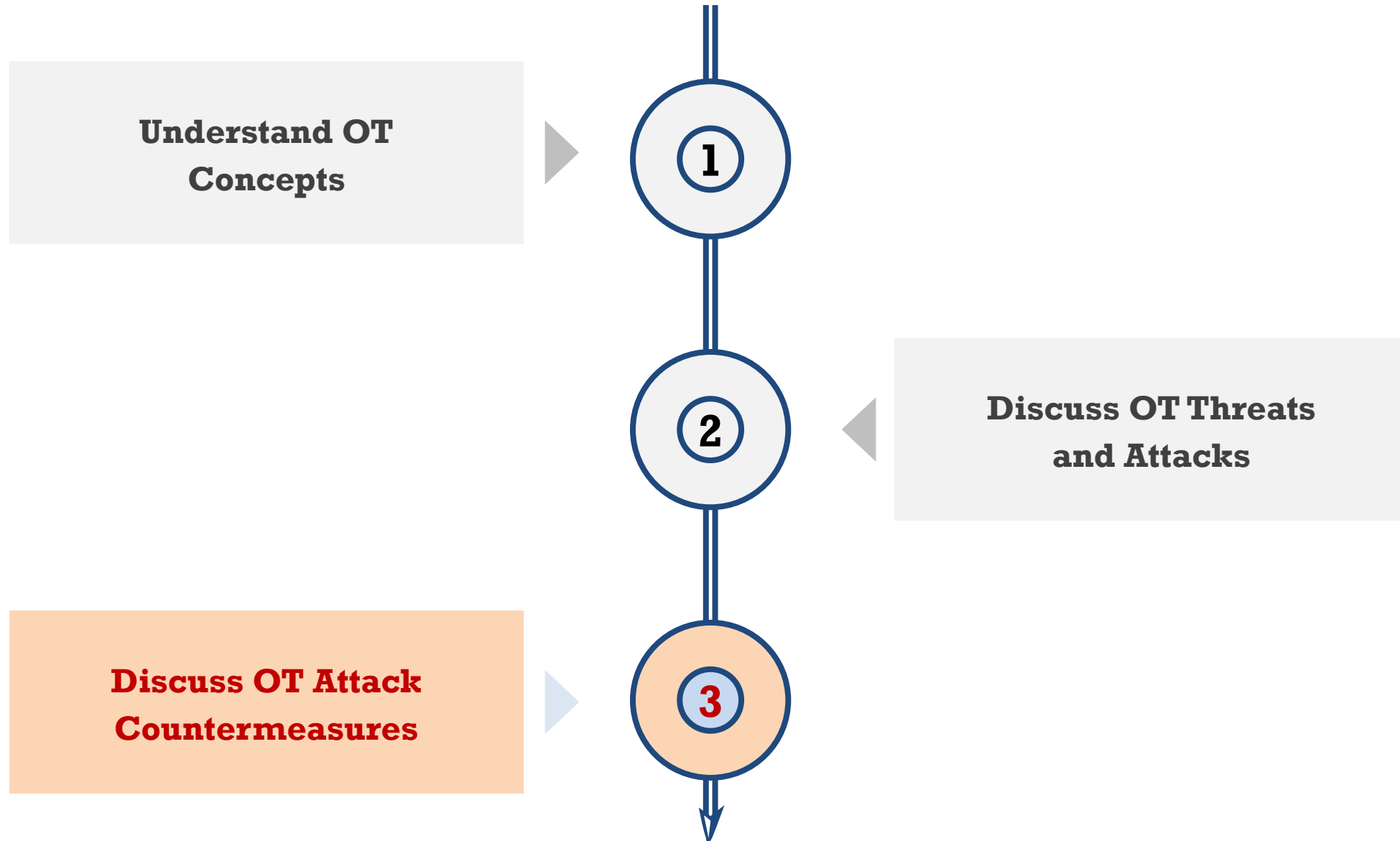


modbus-cli
<https://github.com>



PLCinject
<https://github.com>

Module Flow



OT Attack Countermeasures

1

Use **purpose-built sensors** to discover vulnerabilities in the network

2

Update systems to the latest technologies and regularly **patch systems**

3

Implement secure configuration and **secure coding practices** for OT applications

4

Maintain an **asset register** for tracking and scrutinizing outdated systems

5

Use **strong passwords** and change the default factory-set passwords

6

Secure remote access through multiple layers of defense by implementing **VPNs**

7

Harden the systems by **disabling unused services** and functionalities

8

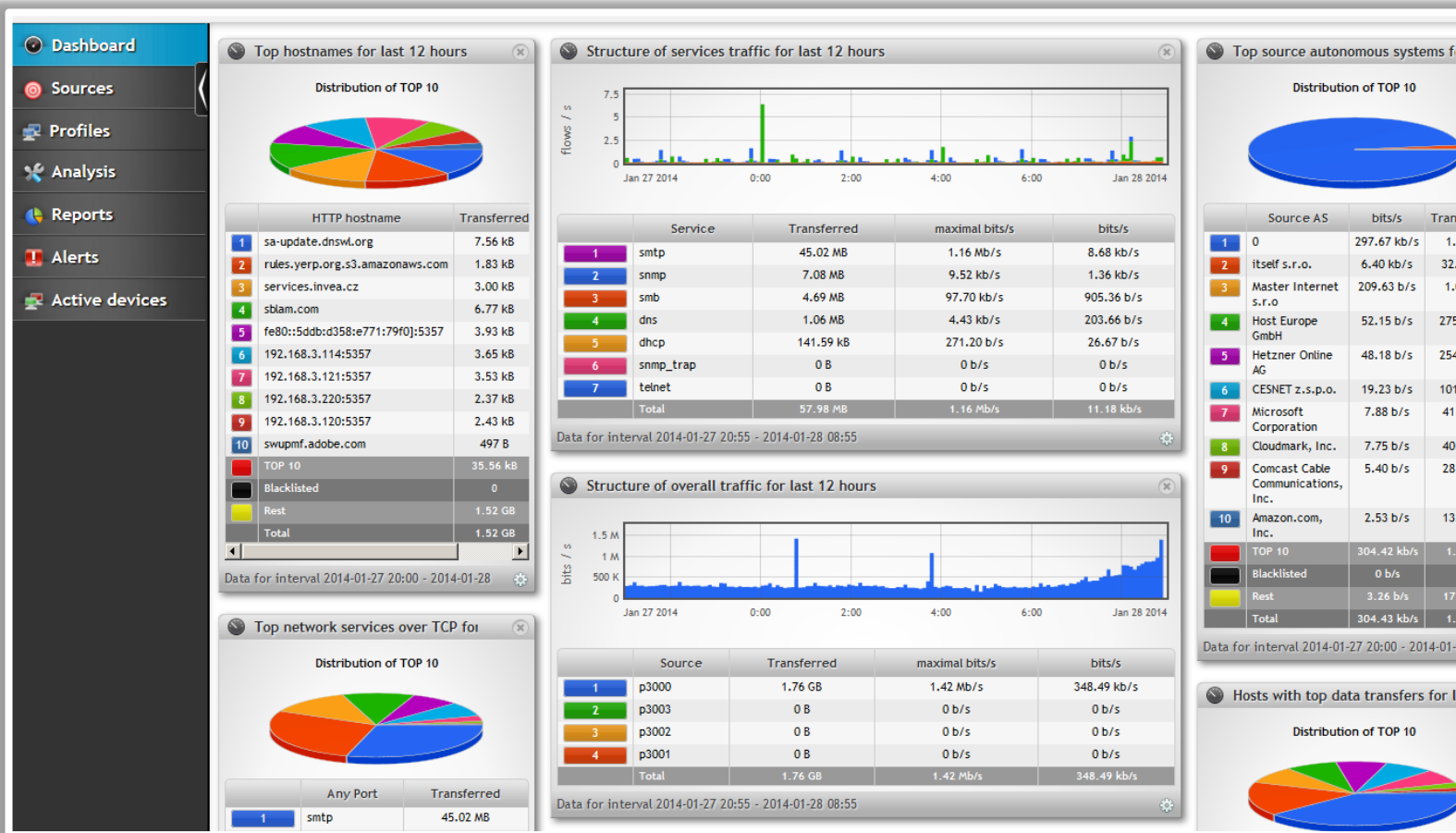
Use only tested and familiar **third-party web servers** for serving ICS web applications

OT Security Tools



Flowmon

Flowmon empowers manufacturers and utility companies to **ensure the reliability** of their industrial networks to avoid downtime and disruption of service continuity



<https://www.flowmon.com>



tenable.ot

<https://www.tenable.com>



Forescout

<https://www.forescout.com>



PA-220R

<https://www.paloaltonetworks.com>



Fortinet ICS/SCADA solution

<https://www.fortinet.com>



Nozomi Networks Guardian™

<https://www.nozominetworks.com>

Module Summary



In this module, we have discussed IoT concepts along with IoT architecture and IoT application areas



We have also discussed in detail various threats to and attacks on IoT networks and devices



This module also illustrated various IoT attack tools



In this module, we have also discussed various countermeasures to be employed to prevent IoT network hacking attempts by threat actors



We have also discussed in detail how to secure IoT networks and devices using IoT security tools



This module also discussed OT concepts along with OT threats and attacks



We have also discussed various countermeasures to defend against OT attacks



This module ended with a demonstration of OT security tools



In the next module, we will discuss in detail on various cloud computing threats and countermeasures

