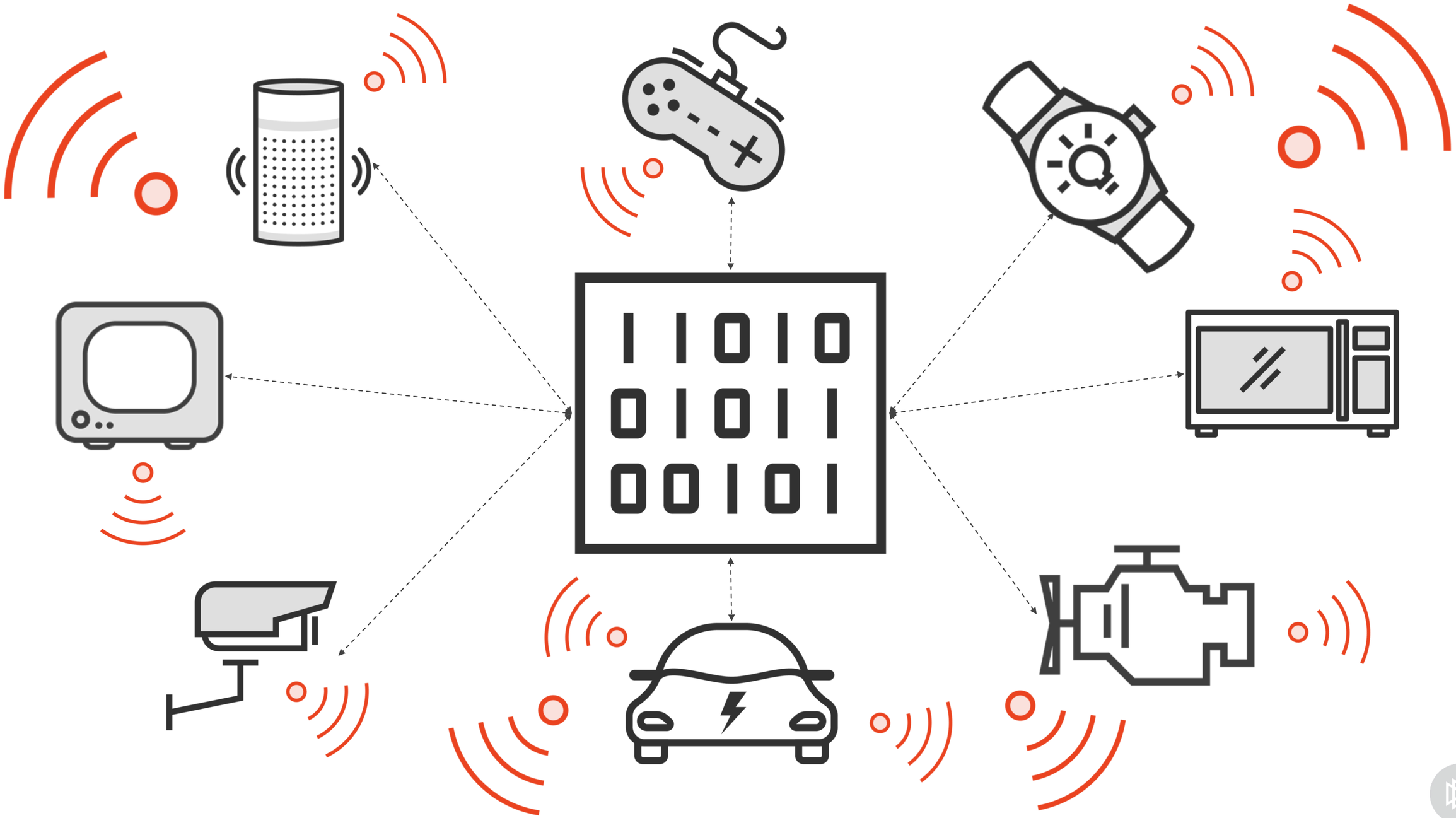
Reviewing IoT and OT Attacks

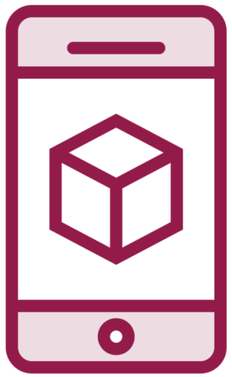
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

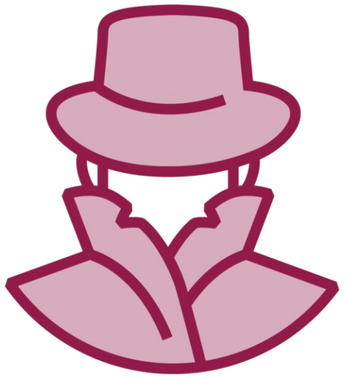
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith

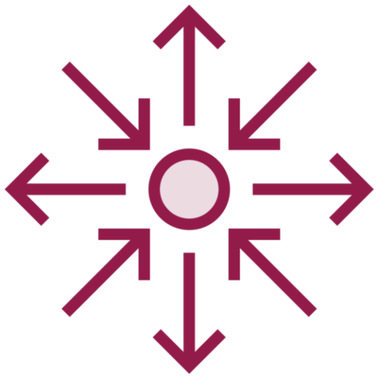


Sensor fusion

The ability to combine information from two completely disconnected sensing devices.







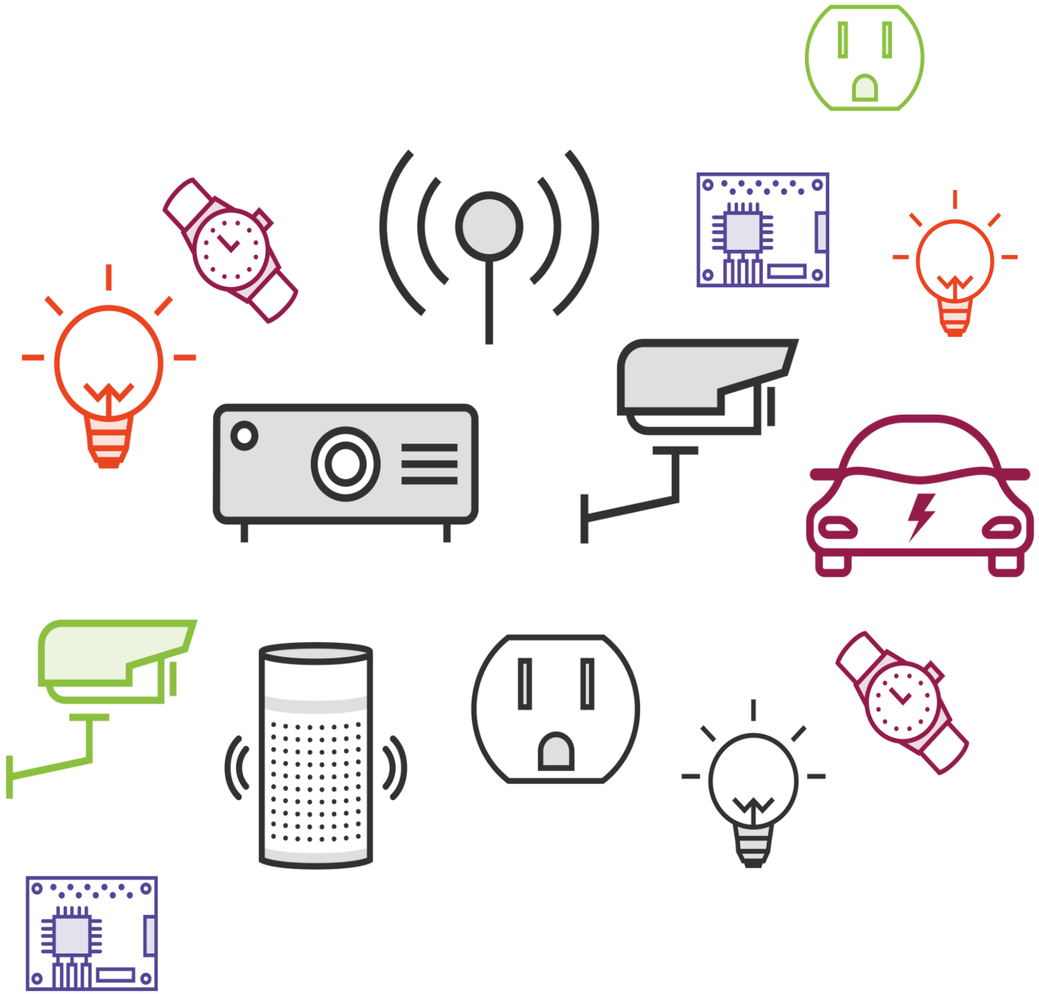
Success Factors

Vulnerability of the targeted system

Ability to exploit that weakness

Integration Issues

Proceed with caution and identify vulnerabilities the devices will bring into your environment



IT and OT teams must be familiar with each other's operations and organizational structure

Information Technology

Personnel and processes

Operational Technology

Benefits of IT and OT Collaborating

- **Enhances security**
- **Enhances efficiency**
- **Enhances quality**
- **Enhances productivity**

IoT Challenges

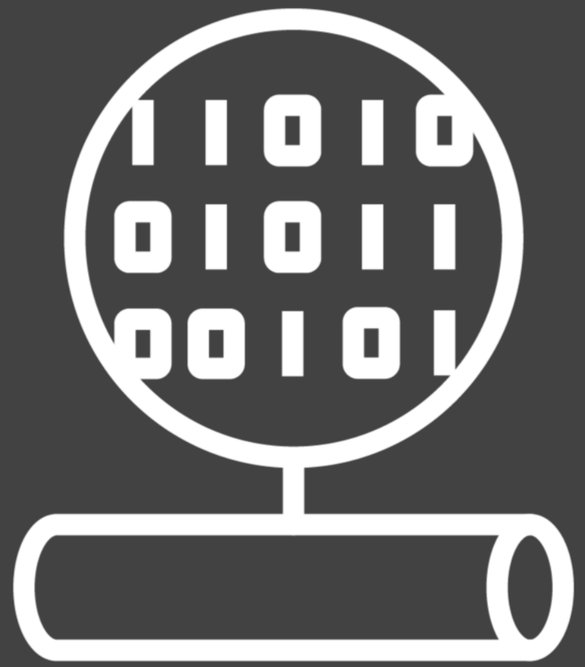
Mobility Challenges

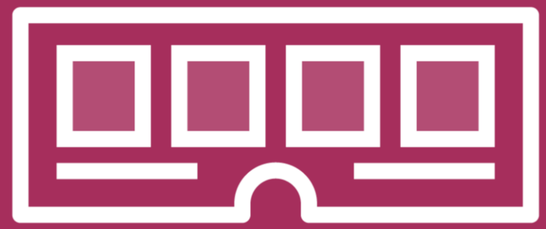
Are they encrypted?

Are we using authentication?

How is our storage security?

What about insecure APIs





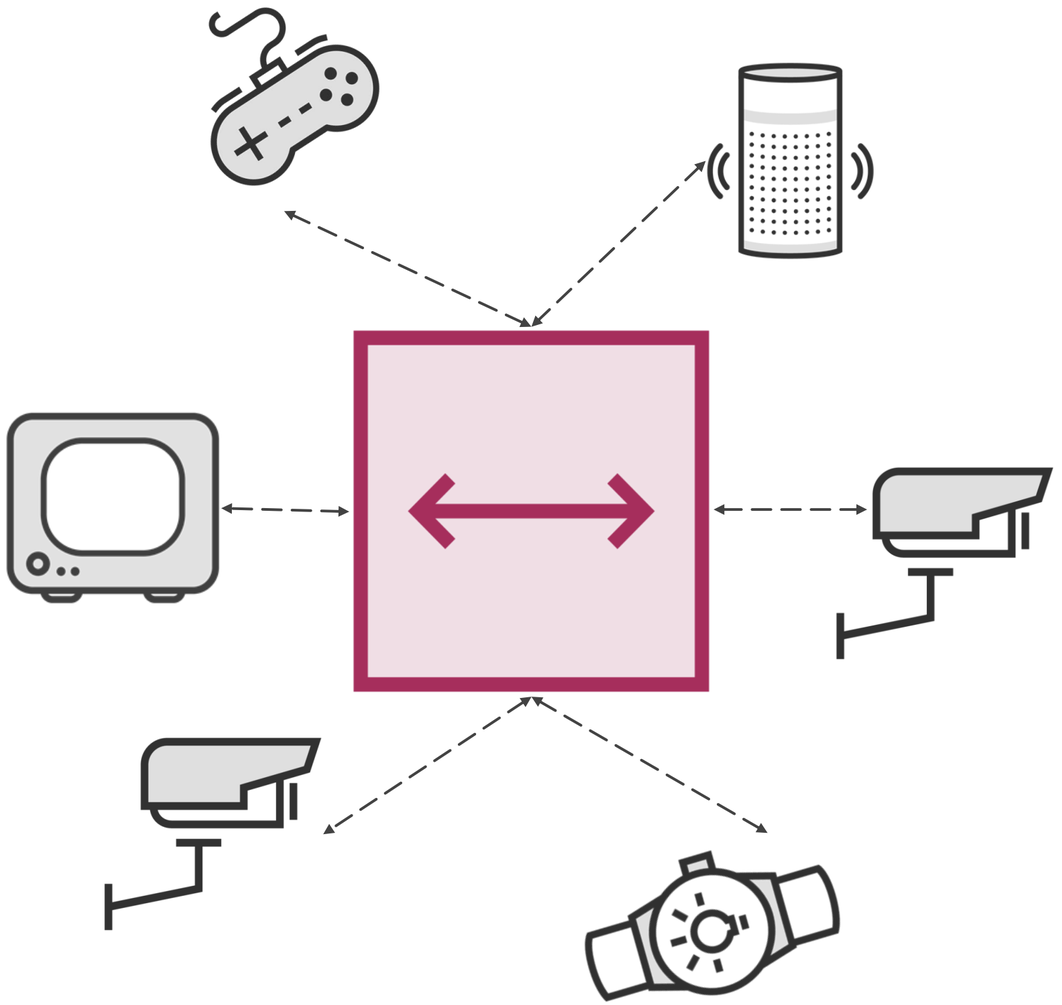
Memory Challenges

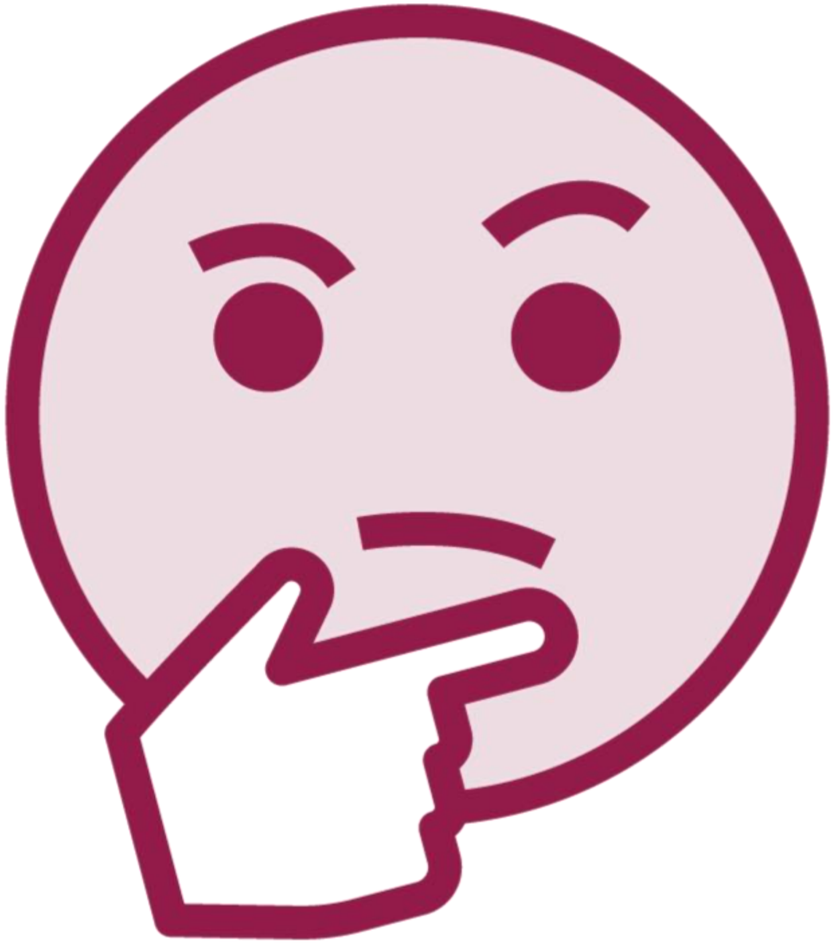
Encryption keys

Credentials

Ecosystem access controls

Authentication keeps malicious devices connecting to your environment





Physical Interface Challenges

User command-line interface

Administrative command-line interface

Web Interface Challenges

Injection

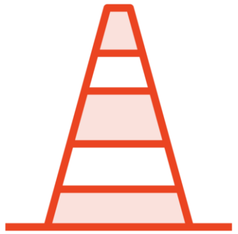
Cross-site scripting

Cross-site request

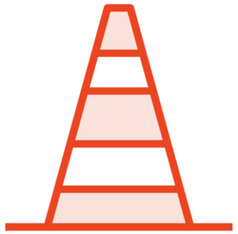
Username enumeration

OT Challenges

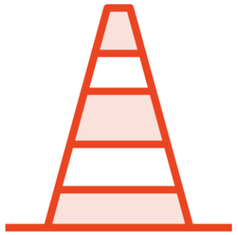
OT Challenges



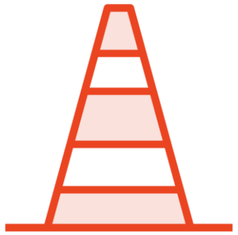
Physical and environmental disaster



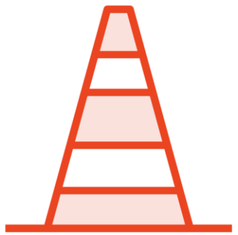
Social engineering



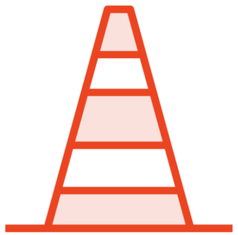
Intentional attacks



Network complexity

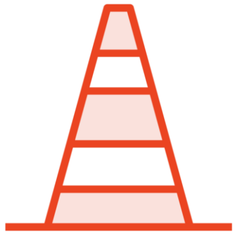


Malicious programs such as viruses and malware

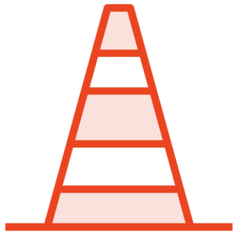


Lack of visibility

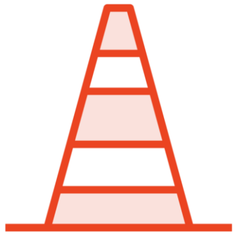
OT Challenges



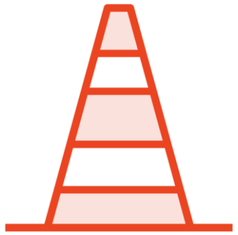
Poor security management



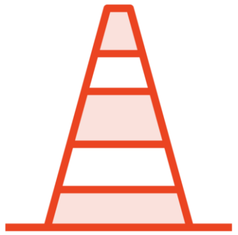
Vulnerable protocols



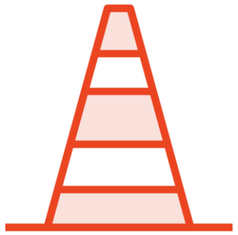
Outdated systems



Security by obscurity



Convergence with IT

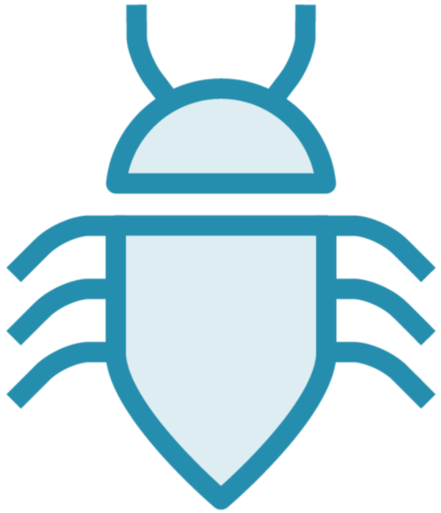


Lack of training and security standards

Industrial Control System Risks and Threats

ICS Risks and Threats

Sniffing and spoofing



Malware attacks

Ransomware attacks

Social engineering

ICS Risks and Threats

Denial of Service

Trojan attacks

Hacked to perform malicious acts

Client-side attacks

Ports Used by ICS/SCADA Systems

Port 80
HTTP

Port 88
UDP

Port 21
FTP

Port 25
SMTP

Port 23
Telnet

Port 161
SNMP

Port 443
HTTPS

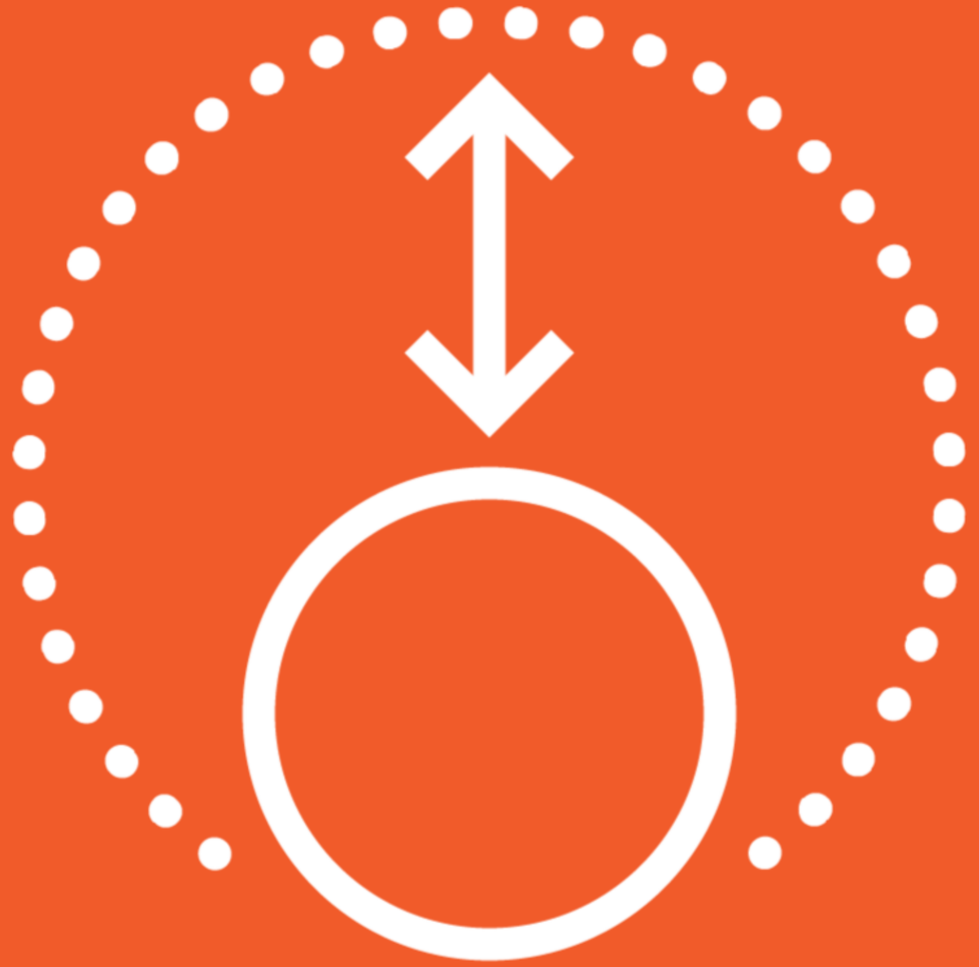
IoT and OT Attacks

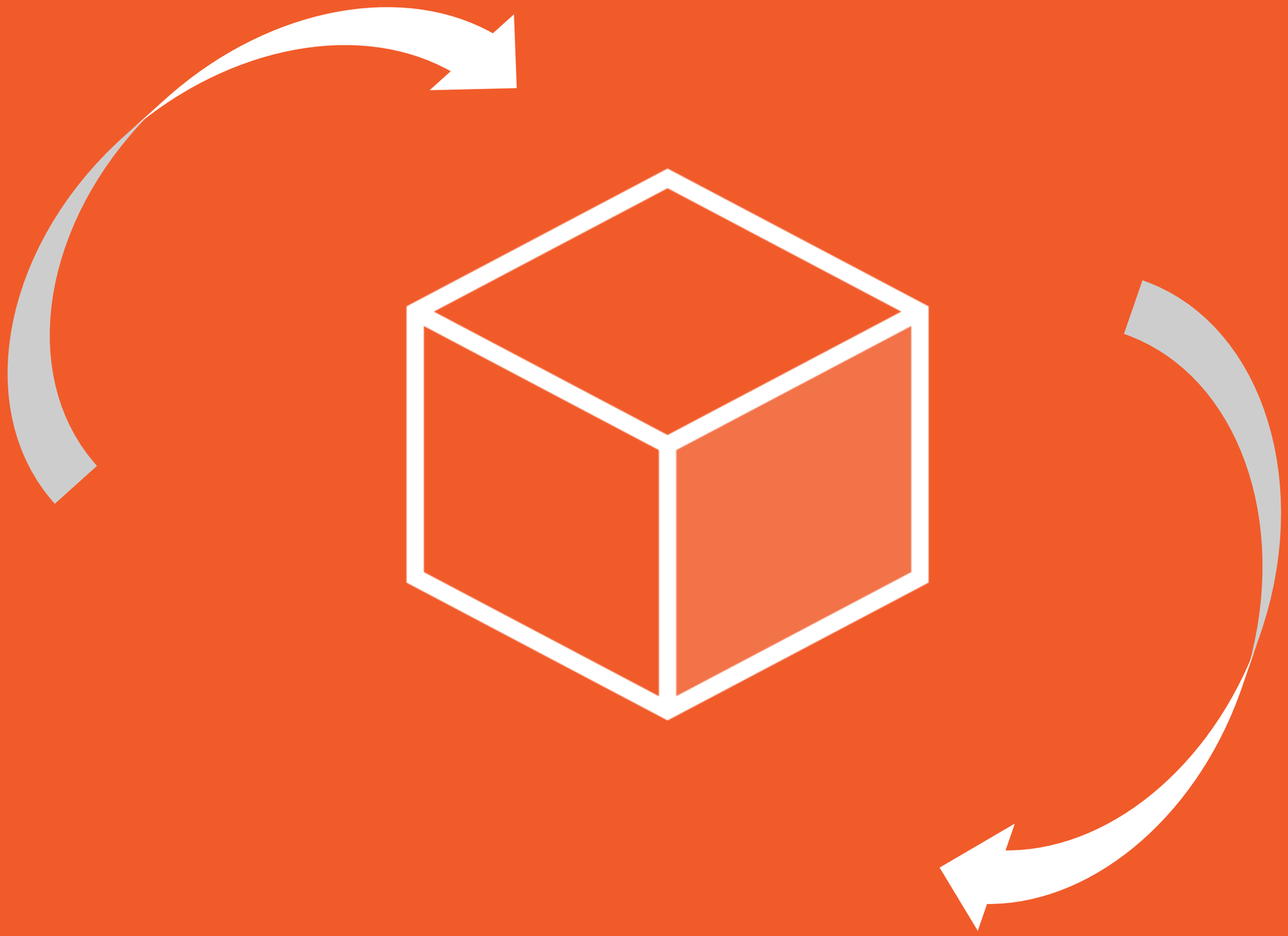
IoT Attacks

Wireless

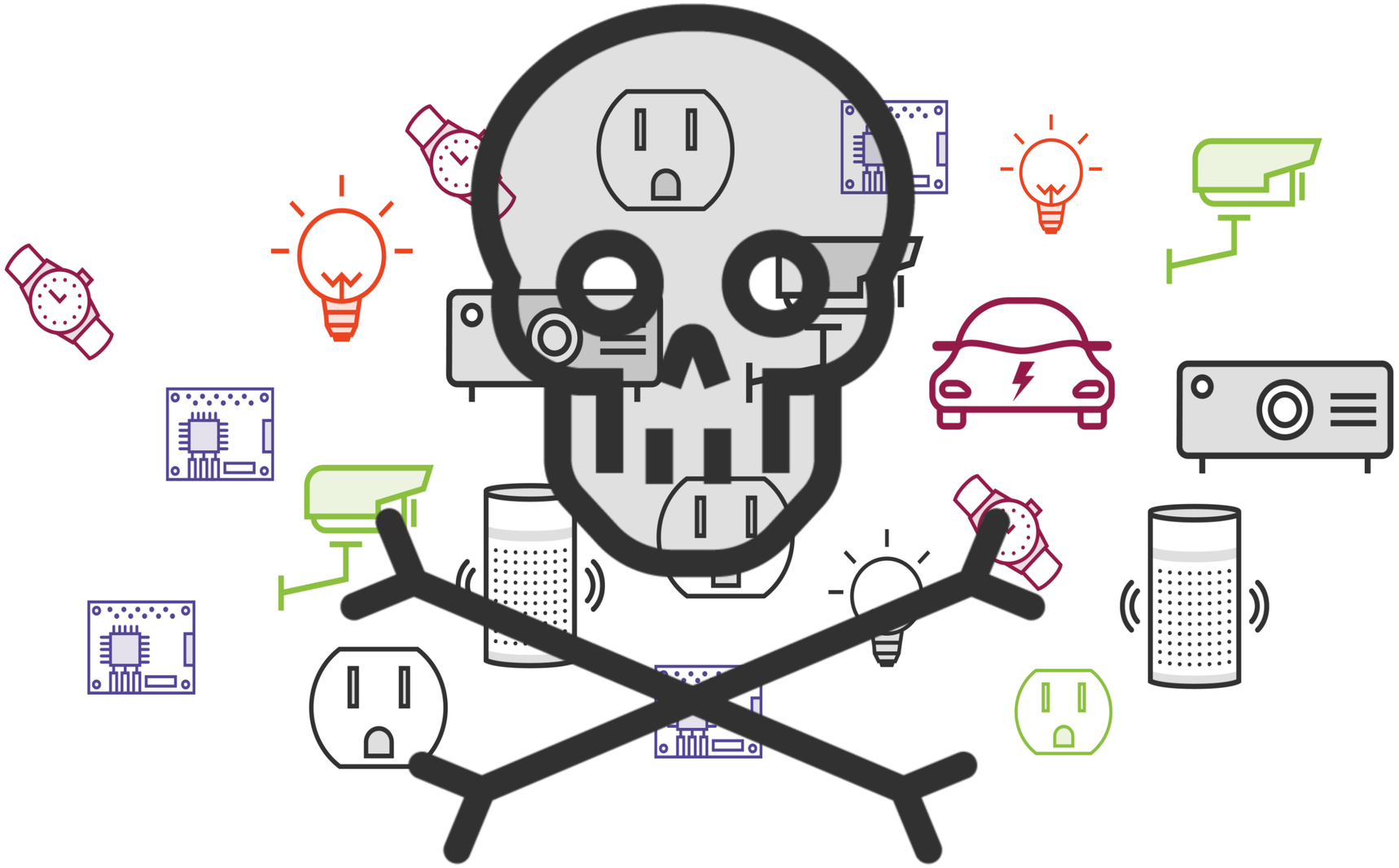
Mobile

Computing

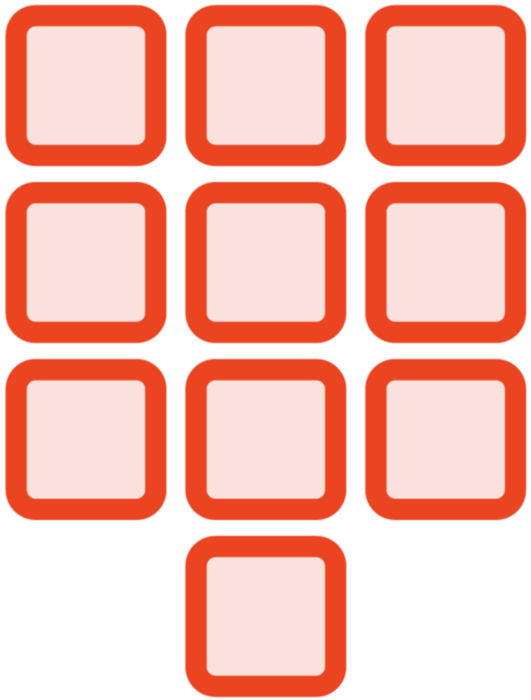


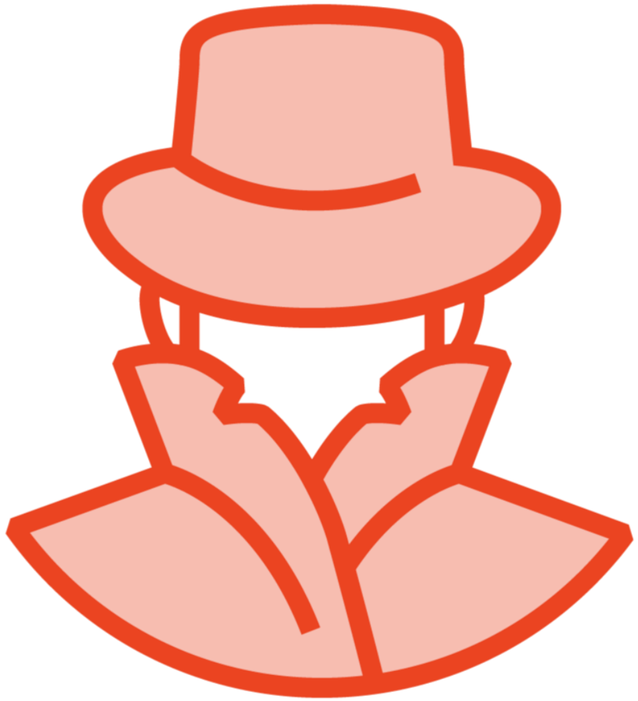


DDoS Attack

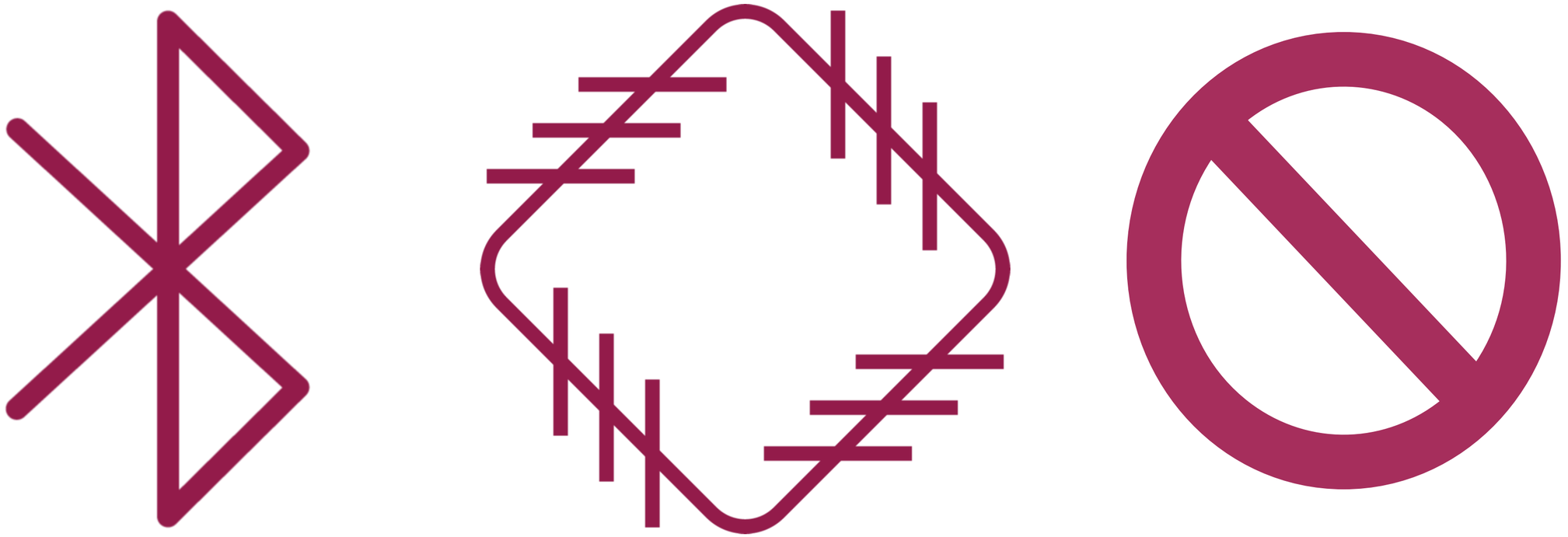


Rolling Code Attack

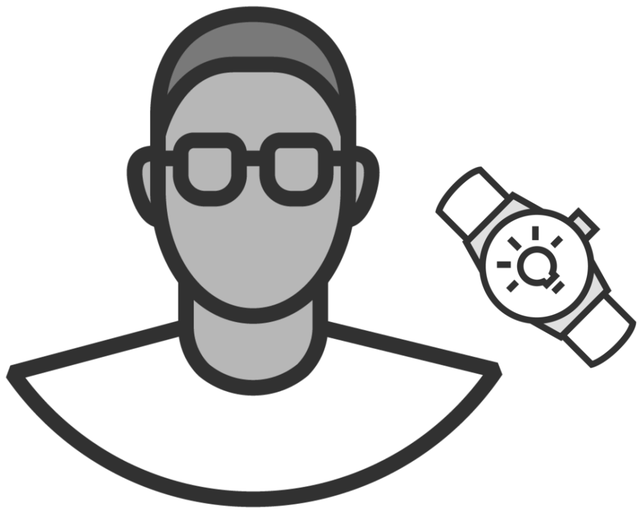


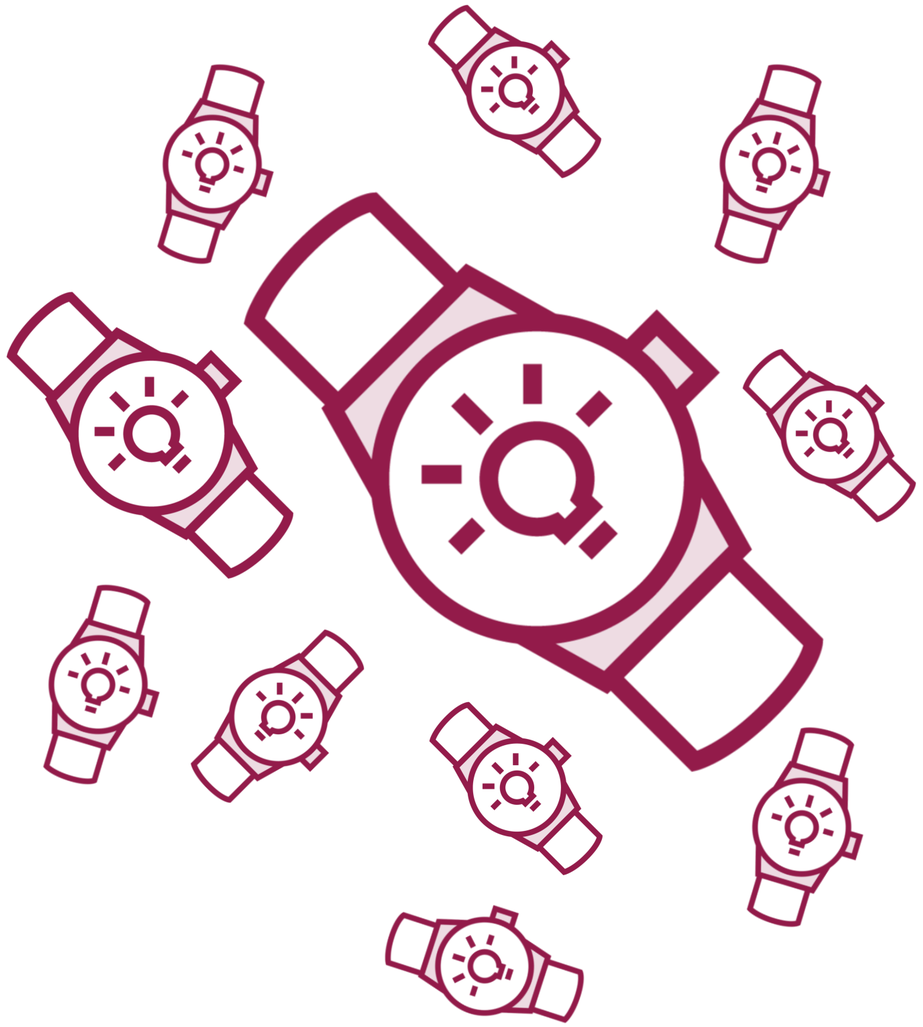


BlueBorne Attack

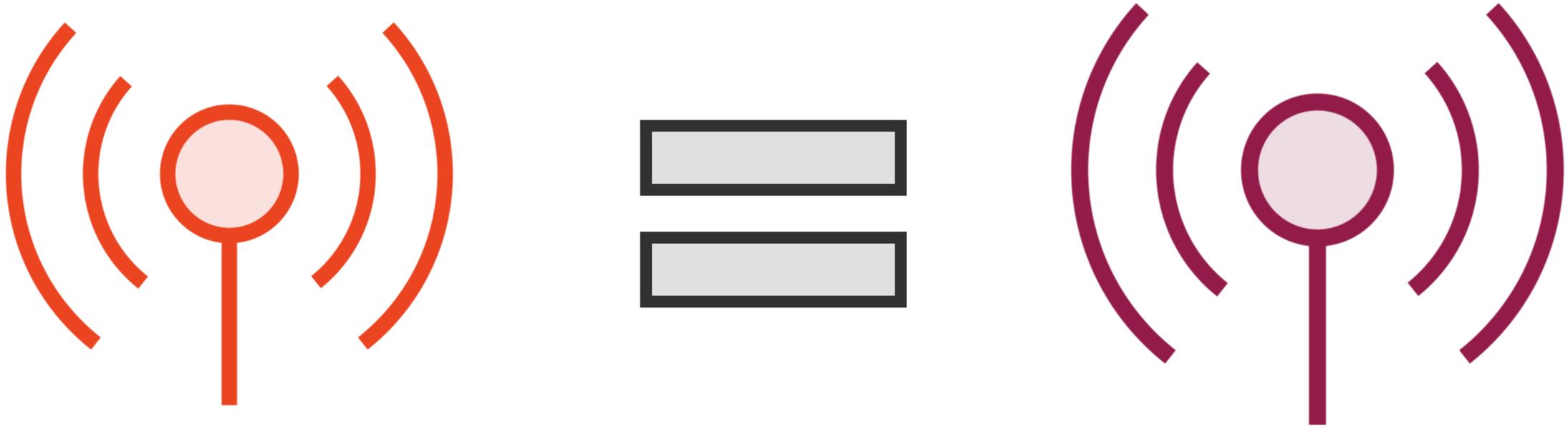


Sybil Attack

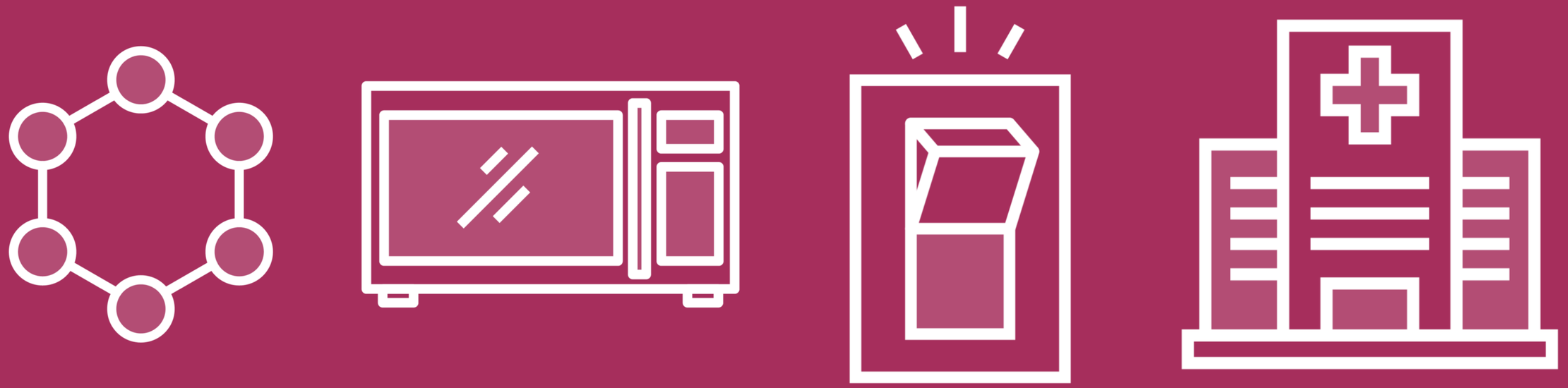




Jamming Attack



Hacking a Smart Grid with a Backdoor



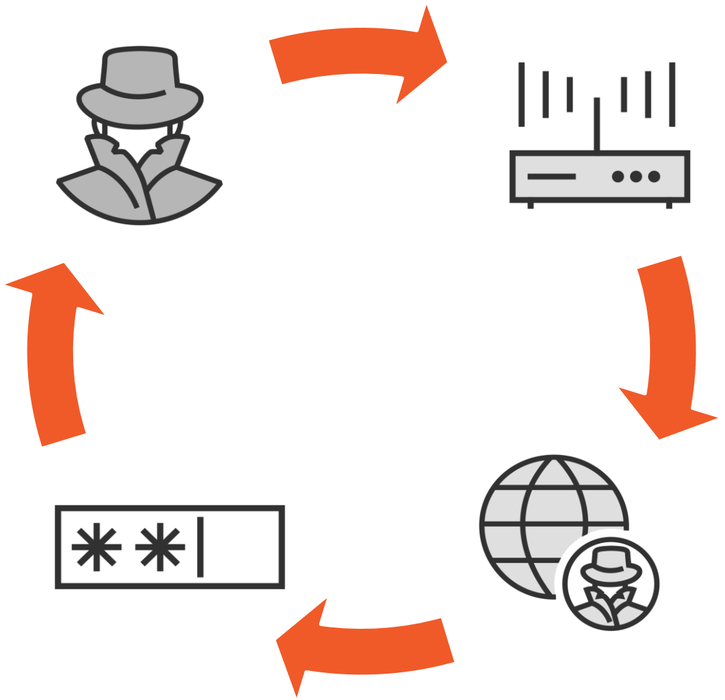
SDR-based Attack

Utilizes software to control radio-frequency hardware

Sends and receives different frequencies within the radio spectrum

Uses both full-duplex and half-duplex modes

DNS Rebinding



DNS entries on the target's router or gateway are altered

OT Attacks

OT Attacks

- HMI-based attacks
- Memory corruption
- Credential Management
- Code Injection
- Side-channel attacks

More Side Channel Attacks

Derives information about cryptographic keys

Power analysis

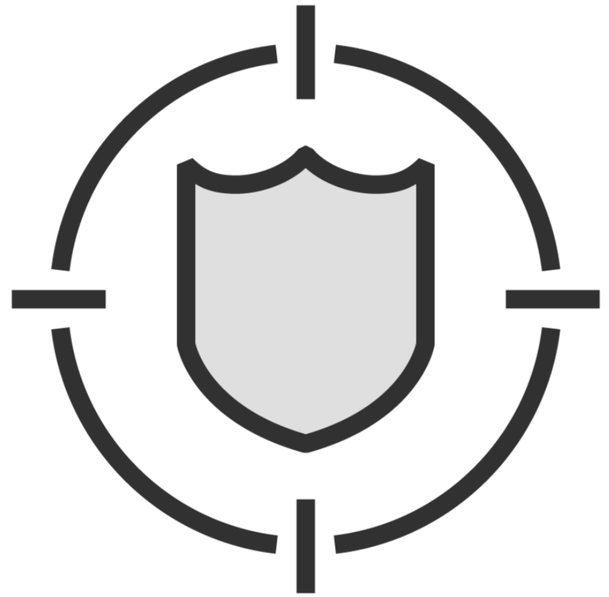
Used with ICS/SCADA systems that run on embedded devices with real time operating systems

Timing analysis

Learning Check

Learning Check

- Device memory attacks
- Physical interface attack
- Outdated systems
- Rolling code attacks
- SDR-based attacks



Up Next:

Understanding IoT and OT Hacking Methodologies