Chapter - 18

IoT & OT Hacking

IoT

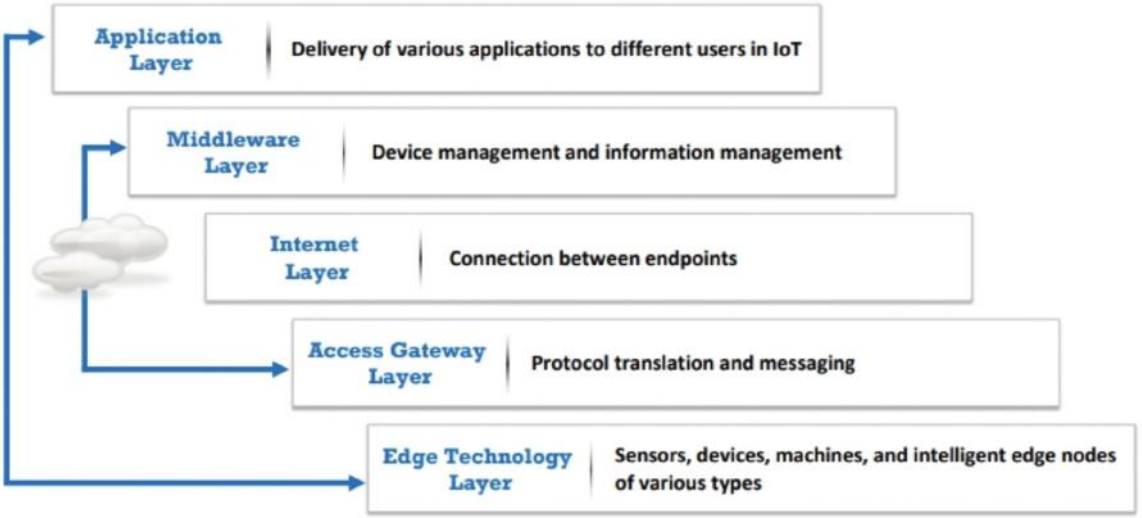
Concepts

- Internet of Things / Internet of Everything.
- devices with IP addresses.
- Capable of sense, collect, send data.

Figure 18.2: Workings of the IoT

Architecture

Application – Middleware – Internet – Gateway – Edge



Protocols & Technologies:

Short-range Wireless Communication

- Bluetooth Low Energy (BLE)
- Light-Fidelity (Li-Fi)
- Near Field Communication (NFC)
- QR Codes and Barcodes
- Radio Frequency Identification (RFID)
- Thread
- Wi-fi
- Wi-Fi Direct
- Z-wave
- ZigBee
- ANT

Medium-range Wireless Communication

- Ha-Low
- LTE-Advanced
- 6LoWPAN
- QUIC

Wired Communication

- Ethernet
- Multimedia over Coax Alliance (MoCA)
- Power-line Communication (PLC)

Long-range Wireless Communication

- Low-power Wide-area Networking (LPWAN)
  - LoRaWAN
  - Sigfox
  - Neul
- Very Small Aperture Terminal (VSAT)
- Cellular
- MQTT
- NB-IoT

IoT Operating Systems

- Windows 10 IoT
- Amazon FreeRTOS
- Contiki
- Fuchsia
- RIOT
- Ubuntu Core
- ARM mbed OS
- Zephyr
- Nucleus RTOS
- NuttX RTOS
- Integrity RTOS

IoT Application Protocols

- CoAP
- Edge
- LWM2M
- Physical Web
- XMPP
- Mihini/M3DA

Attacks

OWASP - Top 10 IoT Threats

- Weak, guessable, hardcode passwords
- Insecure Network Services
- Insecure Ecosystem Interfaces
- Lack of Secure Update Mechanisms
- Use of insecure / outdated components
- Insufficient privacy protection
- Insecure data transfer & storage
- Lack of device management
- Insecure default settings
- Lack of Physical hardening

OWASP IoT Attack Surfaces

- Ecosystem
- Device Memory
- Device Physical Interfaces (CLI)
- Device Web Interfaces
- Device Firmware
- Device Network Services
- Admin Interface
- Local Data Storage
- Cloud web Interface
- Third party backend APIs
- Update Mechanism
- Mobile Application
- Vendor Backend API

- ecosystem Communication
- Network traffic
- Authentication, Authorisation,
- Privacy.
- Hardware (sensors)

IoT Threats

- DDoS
- HVAC System
- Rolling Code
- Blueborne
- Jamming
- Remote Access
  - Backdoor
  - Telnet
- Sybil
- Exploits
- MITM
- Replay
- Forged Malicious device.
- Side channel attack
- ransomware
- client impersonation

- SQL Injection
- SDR attack
- Fault Injection
- Network Pivoting
- DNS Rebinding.

Rolling code - jams & sniffs signal to obtain code.

Blueborne - exploit bluetooth protocol.

Sybil - multiple forged identity to create traffic congestion.

SDR attack - software based radio communication

Fault Injection - introduce fault behaviour, exploit faults to compromise

DNS rebinding - access router using JS code.

DDoS

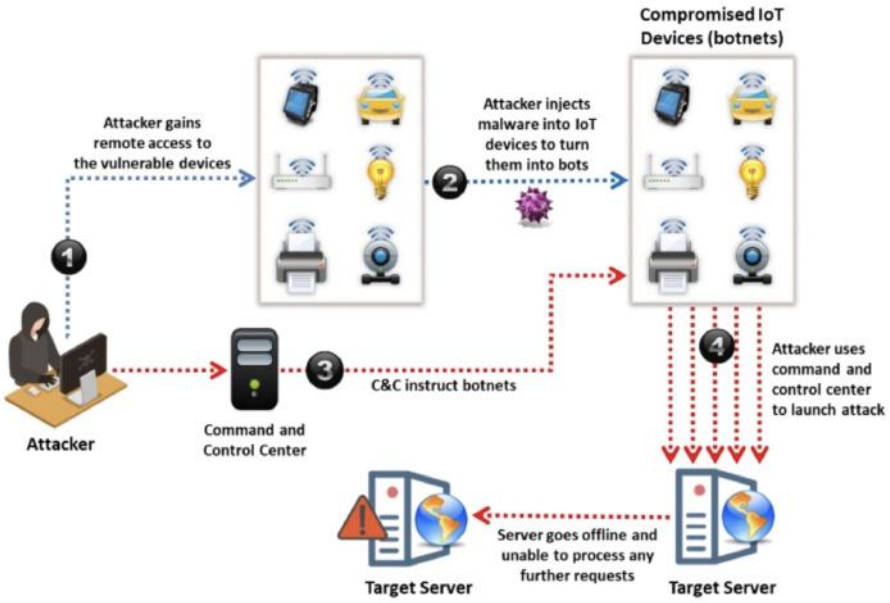


Figure 18.9: DDoS attack on IoT devices

HVAC

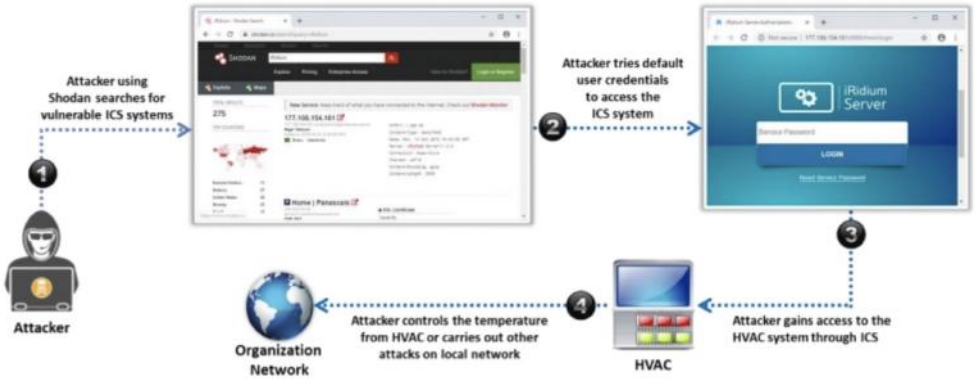


Figure 18.10: Exploiting HVAC system

Rolling Code (Hopping Code)

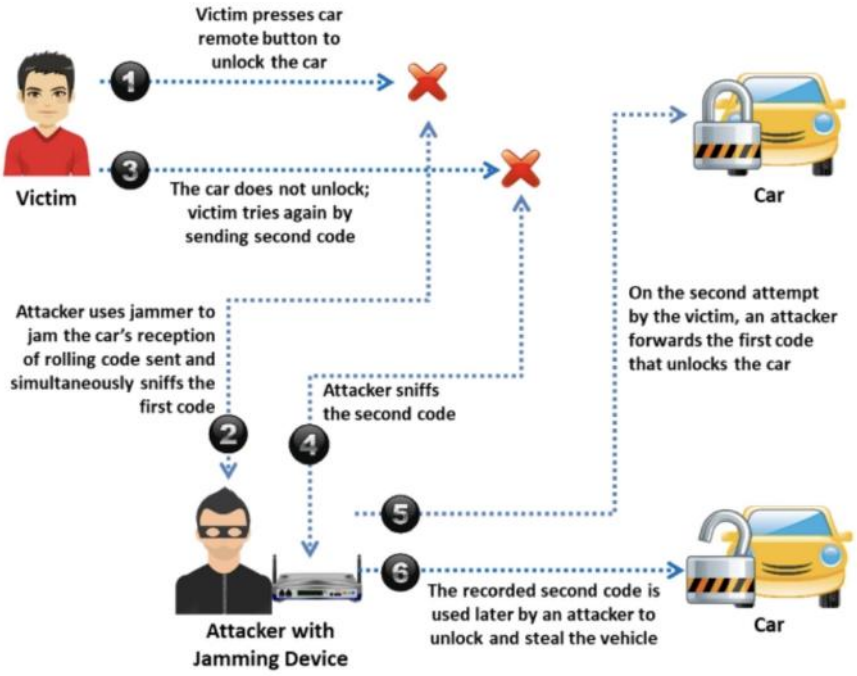


Figure 18.11: Illustration of rolling-code attack

Blue Borne Attack

- Bluetooth to gain access & control.
- Various technique of Bluetooth vulnerability.
- Can penetrate corporate network using exploited device.

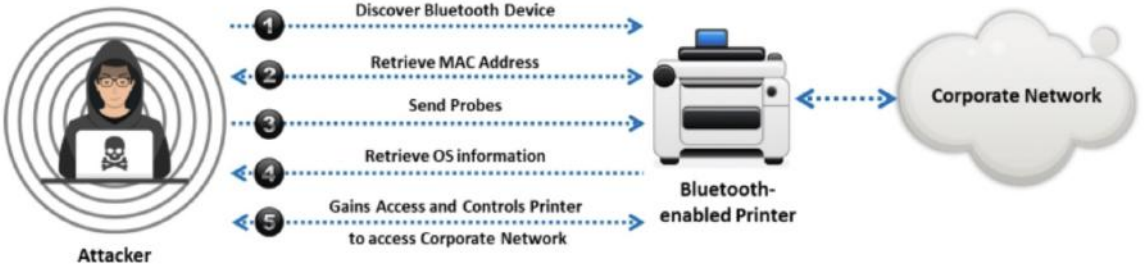


Figure 18.12: Illustration of BlueBorne attack

Smart Grid - Backdoor remote Access

- Social engineering → gather info.
- phishing email → backdoor.
- attacker gains private network.

Figure 18.14: Hacking a smart grid to gain remote access

SDR Attack

- Software defined Radio
- examines signals & sends spam content
- changes transmission / reception of signals.

Replay attack (sniffs commands, injects it)

Cryptanalysis (capture original signal)

Reconnaissance (investigate chipset, discover product)

Fault Injection: (Perturbation Attack)

- injects faulty / malicious program into system
- both invasive & non-invasive.

Types:

- Optical, EM, Body Bias Injection.
- Power / clock / Reset Glitching
- Frequency / Voltage Tampering
- Temperature Attacks.

Dyn Attack (Mirai)

1. Infects device, Populate other devices, create botnets
2. protect itself,
3. Launches Attack

IoT Hacking Methodology

Information gathering

- Shodan (router, camera, server, smart home)
  - use filters like location, city.
- Multiping (find IP address of IoT device)
- FCC ID Search (granted Certification)
  - Grantee ID } components
  - Product ID }
- IoTSeeker (device - default credentials)

Vulnerability Scanning

- Nmap → identify open ports, service.
- RIoT Vulnerability Scanner. (≈ Nessus)

- Foren6 (sniff traffic – GUI)
- Wireshark
- Analyzing Spectrum, IOT Traffic
  - Gnuradio
  - IoT Inspector (analyse network traffic)

Exploitation

- RFCrack. (rolling code)
- Attify Zigbee Framework. (Zbstumbler)
- HackRF One.
  - replay attack, blueborne
- RTL-SDR, GNU Radio (software)
  ↳ (Hardware) } SDR

- Chip Whisperer (sidechannel attack)
  - opensource toolchain → hardware
  - extract cryptographic keys.
- Telnet → Shodan, Censys (remote access)

Maintain Access

- exploit firmware, maintain access
  (Firmware Mod kit)
  ↳ easy reconstruction/deconstruction
- Firmware Analysis
- Reverse Engineering

Hacking Tools

- Censys
- Thingful
- Suphacap

} (Information Gathering)

- beSTORM (Vulnerability Scanning)
- Universal Radio Hacker (SDR)
- Firmalyser Enterprise (Security assessment)

Security Tools

- SeaCat.io (SaaS → operates IoT Solution)
- DigiCert IoT Security Solutions (PKI based)

OT

Concepts

- OT → transfer information (hardware, software)
- detects / causes changes in operations.

OT → (group of ICS)

- SCADA
- RTU
- PLC
- DCS

IIOT (IT/OT Convergence)

- integration of IT & OT systems to improve security, efficiency, productivity.

- Smart Manufacturing (Industry 4.0)

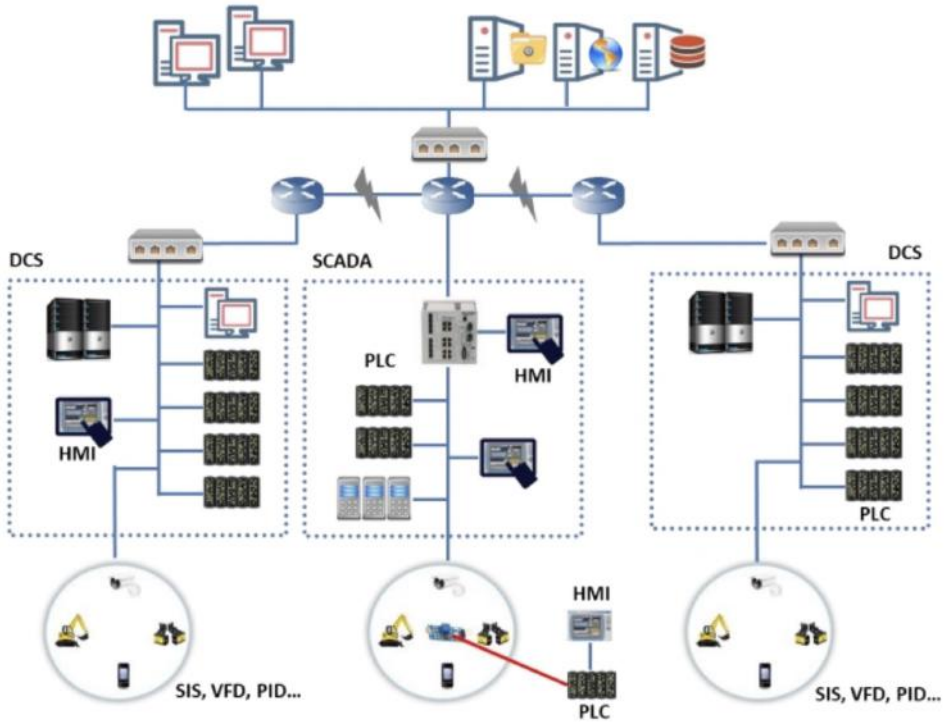
Purdue Model

- PERA Model (Internal connections, dependencies → ICS)
- 3 Zones:
  - Manufacturing zone (OT)
  - Enterprise zone (IT)
  - Demilitarised zone (DMZ)

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

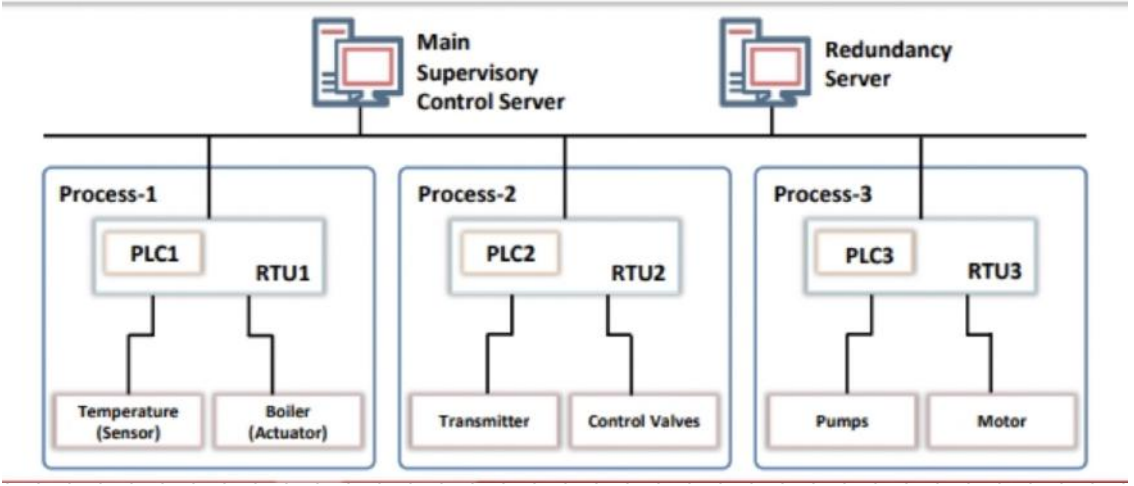
ICS

- Collection of control systems
- Configured in 3 modes:
  - Open loop
  - closed loop
  - Manual mode



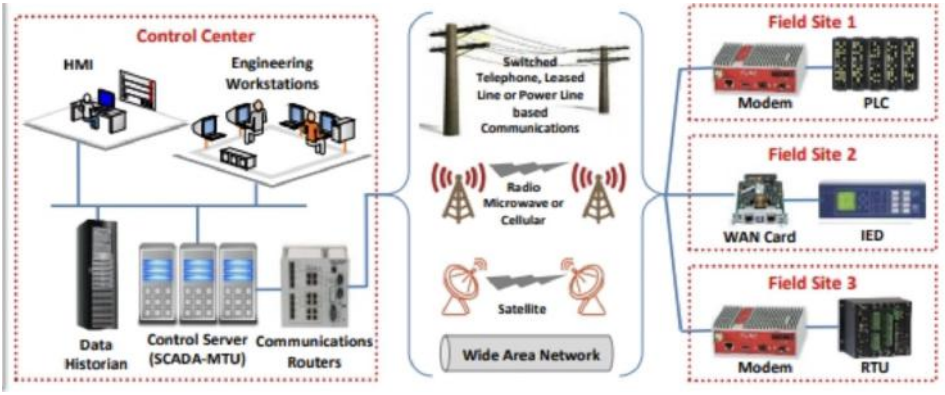
DCS SCADA

- Distributed Control System
- highly engineered, large Scale Control system
- Performs industry tasks
- operated → centralised Supervisory loop (SCADA, MTU) → localised controller (RTU / PLC)



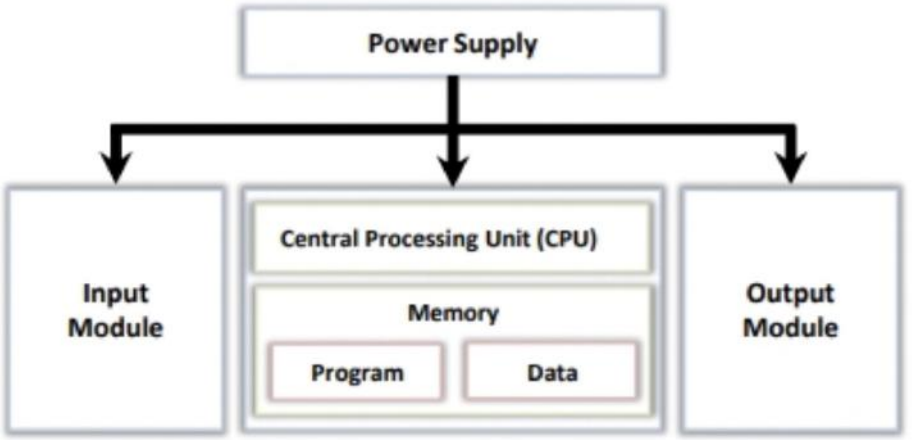
SCADA

- Centralised supervisory control system
- control, monitor industry infrastructure.
- integrates data acquisition system, data transmission system, human machine interface (HMI)
- Consists of:
  - Control Server (SCADA-MTU)
  - communication devices.
  - PLC, RTU.



PLC

- Programmable logic Controller.
- Perform task using custom instructions.
- Consists of:
  - CPU Module
  - Power Supply
  - I/O Modules.



BPCS

- Basic Process Control System
- Process control, Monitoring Infrastructure.
- responds to input signals.

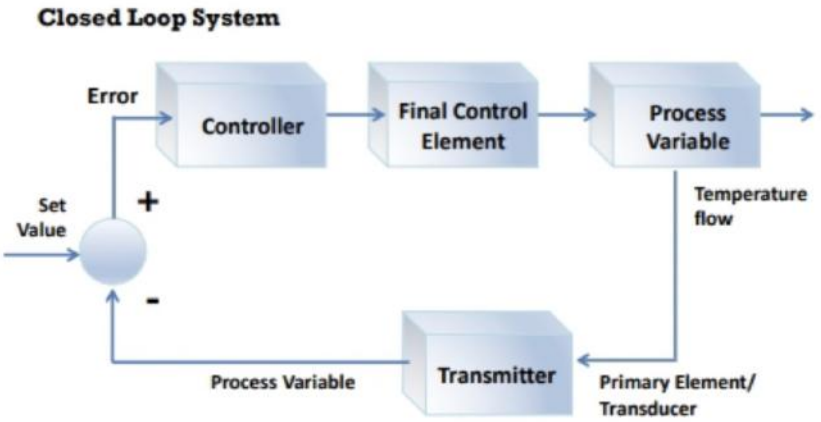
↓

generates output signals.

↓

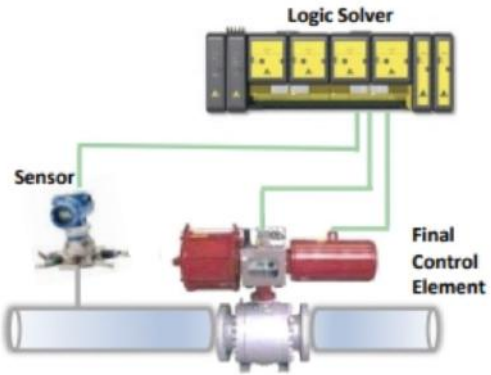
operate on approved design strategy

Basic Process Control System



SIS

- Safety Instrumented Systems
- Safeguard manufacturing environment from hazardous incident.
- risk management strategy.
- Consists of:
  - Sensor, (collect, Process Parameter)
  - logic solver, (execute actions)
  - final control element. (bring safe state)



OT Attacks

HMI-based attack

- attackers compromise the Core hub → HMI
- It controls critical infrastructure.
- causes physical damage to SCADA.

Memory Corruption

Credential Management

Lack of AA & defaults

Code Injections.

PLC Attack

- PLC controls physical processes

- exploits PIN control operations.

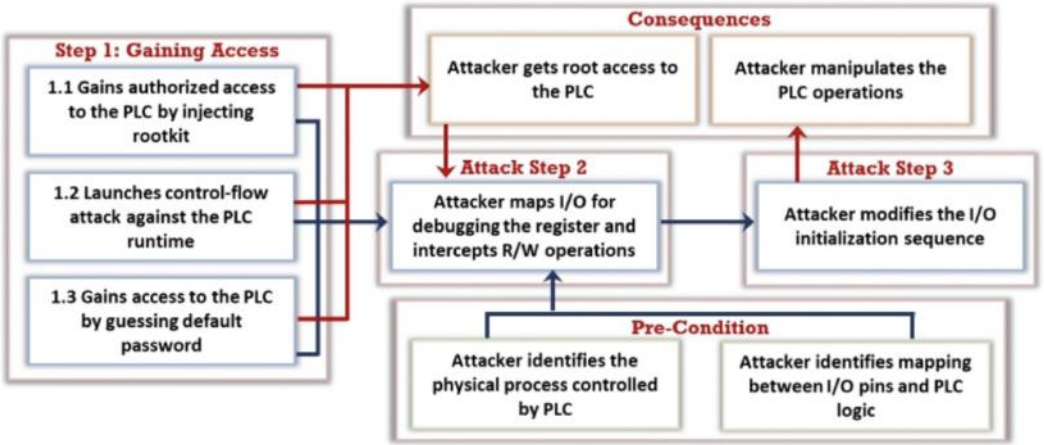


Figure 18.72: Hacking PLC through PLC rootkit attack

Hacking Industrial System

- replay attack (record, replay commands)
- Command Injection. (alter RF Packets)
- repair Malicious RF Controller.
- Malicious reprogramming attack.

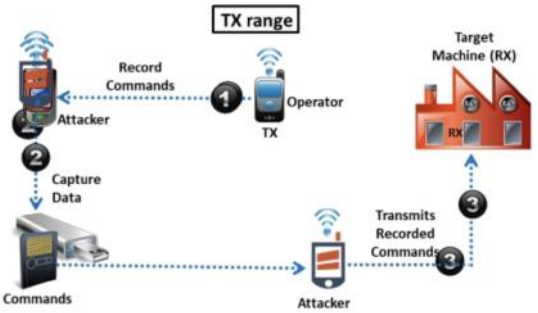


Figure 18.73: Replay attack on industrial systems

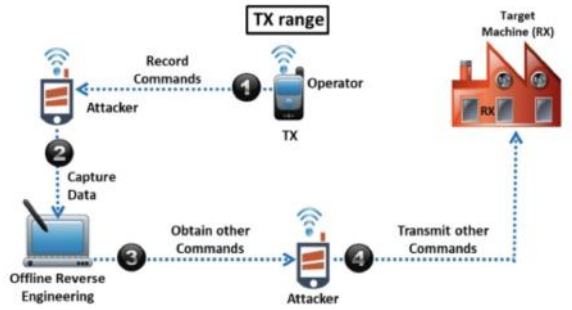


Figure 18.74: Command injection attack on industrial systems

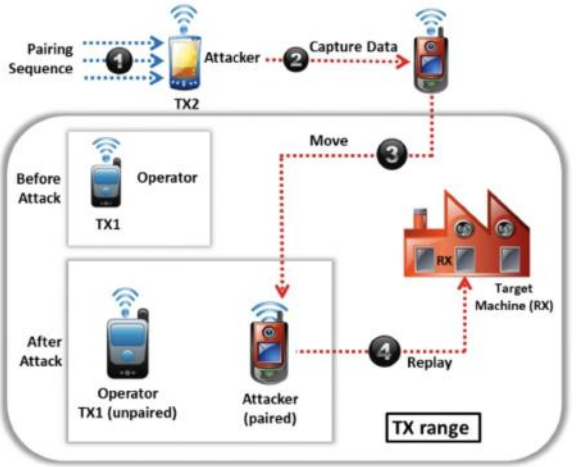


Figure 18.76: Malicious re-pairing attack on an industrial machine

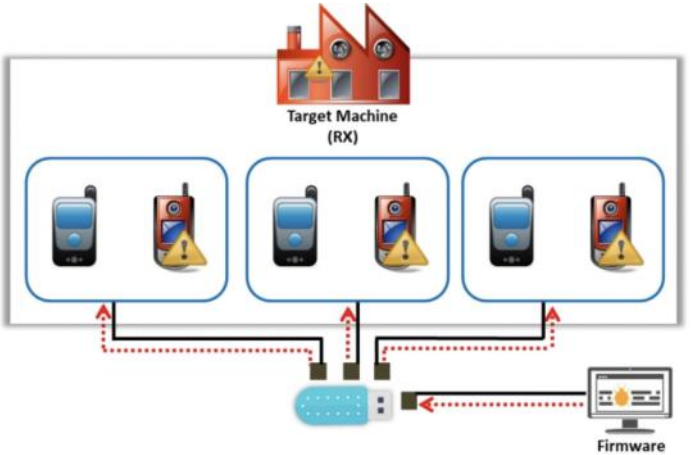


Figure 18.77: Malicious reprogramming attack on an industrial machine

OT Malware

- Mega Cortex (ransomware)
  - ↳ done using trojan downloaders.
- LockerGroga (ransomware)
  - ↳ need admin privilege.

1. initial execution
2. Running Master process
3. Running Slave process.
4. Ransom Note.

Hacking Methodology

Information Gathering

- Shodan.
- Default password → CRITIFENCE
- Nmap Scanning
- SCADA shutdown tool (enumerate slave)

Vulnerability Scanning

- Nessus.
- Skybox Vulnerability Control.
- Network Miner (sniffing)
- Wireshark (TCP traffic (Modbus)

↳ GRASSMARLIN (Topology)

Launch Attacks

↳ Metasploit (Modbus slaves)

↳ Modbus-cli (PLC attack)

1. read register values.
2. read coil values.
3. Manipulate those values.
4. Capture data → output file.

↳ DNP3 (remote Access)

Hacking Tools

- Search Diggity

- SmartRF Packet Sniffer.
- Vulnerability Scanning → CyboX
- ICS exploitation Framework.

Secure Controls - Purdue Model

Zone	Purdue Level	Attack vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, industrial spying, unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems & Basic Controls)	DoS exploitation, Unencrypted protocols, Default credentials, Application and OS vulnerabilities	Altering industrial process, industrial spying	IPS, Firewall, Communication encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption in the physical process	Point to point communication, MAC authentication, additional security gateways at level 1 & 0

Security Organisation

↳ OTCSA (technical awareness)

↳ OT-ISAC (share threat info)

↳ IOTSA (identify, mitigate threats)

OT Security Solution

- Firewall (monitor, control)
- Unified Identity, OT Access Management
- Asset Inventory, Device Authorisation.
- OT Network Monitoring, Anamoly detection
- decoys to deceive attackers. (honeypots)

Security Tools

- Flowmon (avoid downtime)