**Module 18: IoT and OT Hacking**

**Concepts**

* How the IoT works
  + Sensing technology
  + IoT gateway: Bridge the gap between an IoT device and the end-user
  + Cloud server/data storage
  + Remote control using mobile app
* IoT architecture
  + Application Layer
  + Middleware Layer
  + Internet Layer
  + Access Gateway Layer
  + Edge Technology Layer

**IoT technologies and Protocols**

* Short-range wireless communication
  + BLE (bluetooth low energt)
  + LIFI (Light-Fidelity)
  + NFC (Near Field Communication)
  + QR CODE AND Barcodes
  + RFID (Radio frequency identification)
  + Thread
  + WIFI
  + Wifi Direct
  + Z-wave
  + ZigBee
  + ANT
* Medium-range wireless communication
  + Ha-Low
  + LTE-advanced
  + 6LoWPAN
  + QUIC
* Wired communication
  + Ethernet
  + MoCA (Multimedia over Coax Alliance)
  + PLC (Power-line Communication)
* Long-range communication
  + LPWAN (Low-power wide-area networking)
  + VSAT (Very small aperture terminal)
  + Cellular
  + MQTT **(Message Queuing Telemetry Transport)**
  + NB-IoT
* OS
  + Win10 IoT
  + Amzon FreeRTPS
  + Contiki
  + Fuchsia
  + RIOT
  + Ubuntu Core
  + ARM mbed OS
  + Zephyr
  + Nucleus RTOS
  + NuttX RTOS
  + Integrity RTOS
* Application Protocols
  + CoAP
  + Edge
  + LWM2M
  + Physical Web
  + XMPP
  + Mihini/M3DA

**IoT Communication Models**

* Device-to-Device model
* Device-to-Cloud model
* Device-to-Gateway model
* Back-end Data-Sharing model

**Challenges of IoT**

* Lack of security and privacy
* Vulnerable web interfaces
* Legel, regulatory, and right issues
* Default, weak, and hardcoded credentials
* Clear text protocols and unnecessary open ports
* Coding errors (buffer overflow)
* Storage issues
* Difficult to update firmware and OS
* Interoperability standard issues
* Physical theft and tampering
* Lack of vendor support for fixing vulnerabilities
* Emerging economy and development issues

**IoT attacks**

* **Application:** validation of the inputted str, AuthN, AuthZ, no automatic security updates, default password
* **Network:** Firewall, improper communication encryption, services, lack of automatic updates
* **Mobile:** Insecure API, lack of communication channel encryption, authentication, lack of storage security
* **Cloud:** improper authentication, no encryption for storage and communication, insecure web interface
* **IoT:** Application+Network+Mobile+Cloud

**OWASP Top10 IoT threats**

* Weak, Guessable, or Hardcoded passwords
* Insecure network services
* Insecure ecosystem interfaces
* Lack of secure update mechanisms
* Use of insecure or outdated components
* Insufficient privacy protection
* Insecure data transfer and storage
* Lack of device management
* Insecure default settings
* Lack of physical harding

**OWASP IoT attack surface area**

* Ecosystem
* Device memory
* Device physical interfaces
* Device web interface
* Device fireware
* Device network services
* Administrative interface
* Local data storage
* Cloud web interface
* Third-party backend apis
* Update mechanism
* Mobile application
* Vendor backend APIs
* Ecosystem communication
* Network traffic
* Authenticatio/Authorization
* Privacy
* Hardware

**IoT Threats**

* **DDoS attack**
* **Attack on HVAC systems**: Heating, Ventilation, and Air conditioning systems have many security vulnerabilites that can be exploited to steal…
* **Rolling Code attack:** Jam and sniff the signal to obtain the code transferred to a vehicle’s receiver
* **BlueBorne attack:** exploit the vulnerabilities of the bluetooth protocol to compromise the device
* **Jamming attack:**
* **Remote access using backdoor**
* **Remote access using telnet**
* **Sybil attack:** Use multiple forged identities to create a strong illusion of traffic congestoin
* **Exploit kit**
* **MITM attack**
* **Replay attack**
* **Forged malicious device**
* **Side channel attack**
* **Ransomware**
* **Client impersonation**
* **SQL injection attack**
* **SDR-based attack:** Software Defined radio is used to examine the communication signals in the IoT network and sends spam content…
* **Fault injection attack:** Perturbation attacks, occur when a perpetrator injects any fault or malicious program into the system to compromise the system security
* **Network privoting**
* **DNS rebinding attack**

**Dyn Attack**

* Mirai is a **piece of malware** that finds the IoT devices and infect them
* Once infected, Mirai adds the infected device to a botnet

**IoT Hacking Methodology**

* Info gathering: **Shodan, MultiPing, FCC ID Search, IoTSeeker**
* Vulnerability scanning
  + Scanning
    - Nmap
    - RIoT Vulnerability Scanner
  + Sniffing:
    - Foren6: Capture **6LoWPAN** traffic
    - Wireshark
  + Analyzing spectrum and IoT Traffic
    - Gqrx (spectrum)
    - IoT inspector (traffic)
* Launch attacks
  + Rolling code attack using **RFCrack**
  + Hacking Zigbee Devices with **Attify Zigbee Framework**
  + BlueBorne attack using **HackRF One**
  + Replay attack using **HackRF One**
  + SDR-Based attacks using **RTL-SDR** and **GNU Radio**
  + Side channel attack using **ChipWhisperer**
* Gain remote access
  + Gain remote access using **Telnet**
* Maintain access
  + Maintain access by **exploiting fireware**

**Fireware analysis and reverse engineering**

* Obtain fireware
* Analyze fireware
* Extract the filesystem
* Mount the filesystem
* Analyze the filesystem
* Emulate fireware

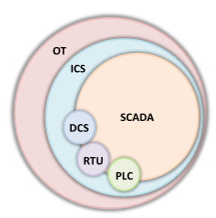
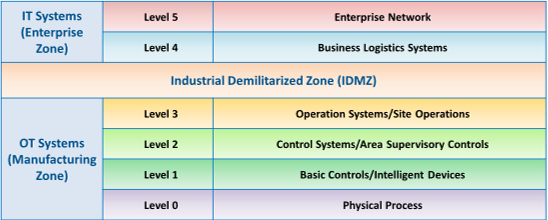
**IoT Hacking tools**

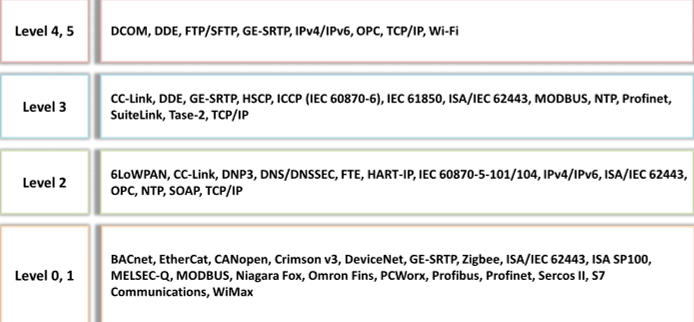
* Info-gathering
  + Censys
  + Thingful
* Sniffing
  + Suphacap
* Vulnerability-scanning
  + beSTORM
* Perform SDR-Based attack
  + **Universal Radio Hacker:** investigate unknown wireless protocols
* **Firmalyzer Enterprise:** perform an automated security assessment

**Countermeasure**

* Defend against IoT Hacking
  + Disable guest and demo user account
  + implement IDS, IPS
  + Using encryption and sue PKI
  + Use VPN
  + Disable telnet
  + Disable UPnP port on routers
  + Monitor traffic on port 48101
  + …
* General guidelines for IoT device manufacturing companies
  + SSL/TLS used for communication
  + Mutual check on SSL certificates, the certificate revocation list
  + Strong password
  + Secure with a chain of trust
  + Implement account lockout mechanism
  + Lock and devices
  + Checking the device for unused tools, using whitelisting to allow…
  + Use secure boot chain
* IoT device management
* security tool: **SeaCat.io, DigiCert IoT Security Solution**

**OT Concepts**

* **Operational technology** is the software and hardware designed to **detect or cause changes in industrial operations** through direct monitoring and controlling of industrial physical devices
* OT consists of **Industrial Control Systems (ICS)** that include **Supervisory Control and Data Acquisition (SCADA)**, **Remote Terminal Units (RTU)**, **Programmable Logic Controllers (PLC)**, **Distributed Control System (DCS)**, etc., to monitor and control the industrial operations
* Essential terminology
  + asset
  + **zones and conduits**: **A network segregation** technique used to isolate the networks and assets to impose and maintain strong access control mechanisms
  + industrial network
  + business network
  + industrial protocols
  + network perimeter
  + electronic security perimeter
  + critical infrastructure
* **IIOT (IT/OT Convergence, Industrial IoT):** the integration of IT computing system and OT operation monitoring system to bridge the gap between…
* **The purdue model:** Derived from the PERA (Purdue enterprise reference architecture) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks
* 
* **ICS:** a collection of different types of control systems and their associated equipment..
  + An ICS consists of several types of control systems like **SCADA, DCS, BPCS, SIS, HMI,PLCs, RTU, IED, etc**
  + Three mode:
    - **open loop:** The 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:** supervisory control and data acquisition
  + **DCS:** distributed control system
  + **BPCS:** basic process control systems
  + **SIS:** safety instrumentation system
  + **HMI:** human machine interface
  + **PLC:** programmable logic controller
  + **RTU:** remote terminal unit
  + **IED:** intelligent electronic device
* OT Technologies and Protocols



**OT Attacks**

* HMI-based attack
  + HMI is the core hub that **controls the critical infrastructure**
  + Gain access to the HMI system to cause **physical damage to the SCADA devices** or collect…
  + SCADA vulnerabilities exploited by attackers to perform HMI-based attacks
    - Memory corruption
    - Credential management
    - Lack of authorization/Authentication and Insecure defaults
    - Code injection
* Side channel attacks
  + Timing analysis
  + Power analysis
* Hacking PLC
  + Tamper with the integrity and availability of PLC system by exploiting **pin control operations**
* Hacking industrial system through RF remote controllers:
  + Replay attack
  + Command injection
  + Re-pairing with Malicious RF controller
  + Malicious Reprogramming Attack
* OT Malware: MegaCortex, LockerGoga Ransomware

**OT Hacking Methodology**

* Information gathering
  + Identify **ICS/SCADA** Systems using **Shodan (port 502)**
  + Gather default passwords using **CRITIFENCE**
  + Scan using **Nmap**
  + Enumerate slave controllers using **SCADA Shutdown Tool,** it is an ICS testing and automation tool
* Vulnerability Scanning
  + Scan using **Nessus**
  + **Skybox Vulnerability Control**
  + Analyze modbus/TCP traffic using **wireshark**
  + Discover ICS/SCADA network topology using **GRASSMARLIN**
* Launch Attacks
  + Hacking ICS hardware
  + Hacking Modbus slaves using Metaslpoit
  + Hacking PLC using modbus-cli
* Gain remote access
  + Using DNP3
* Maintain access

**OT Hacking Tools**

* Info gathering tools
  + SearchDiggity
* Sniffing and vulnerability-scanning tools
  + SmartRF Packet Sniffer
  + CyberX (scanning)
* OT Hacking Tools:
  + ICS Exploitation Framework (ISF)

**Countermeasures**

* International OT security Org
  + OTCSA (Operational Technology Cyber Security Alliance)
* Security Tools: **Flowmon**