Chapter 8
Mobile & IoT

OT (Operational Technology)

- Concepts
  - Assets
  - Zones/Conduits
  - Industrial Network
  - Business Network
  - Industrial Protocols
    - S7
    - CDA
    - CIP
  - Perimeter
  - Critical Infrastructure
- Purdue Model
  - 3 Zones
    - Enterprise Zone (IT)
      - Enterprise Network
      - Business Logic Systems
    - Industrial Zone (IDMZ)
    - Manufacturing Zone (OT)
      - Site Operations
      - Control Systems
      - Basic Controls
      - Physical Processes
- Control Modes
  - Open Loop
  - Closed Loop
  - Manual
- Industrial Control Systems
  - SCADA
  - BPCS
  - RTU
  - DCS
- Tools
  - GDB
  - Radare2
  - OpenOCD
  - IDA Pro

Internet of Things

- Collection of Devices
  - Sensors
  - Software
  - Storage
  - Electronics
  - Example
    - Smartwatch
    - Toothbrush
    - TVs
    - Thermostat
  - VANET
    - Vehicle Ad Hoc Network
    - Used by Vehicles
    - Wireless Vehicle-to-Vehicle Data Exchange
- Architecture
  - Components
    - Sensing Technology
    - IoT Gateways
    - Cloud/Data Storage
  - Operating System
    - ARM mbed OS
    - Riot OS
    - Nucelus RTOS
    - RealSense OSX
    - Ubuntu Core
  - Communication
    - Wireless
      - Device-to-Device
      - Device-to-Gateway
      - Device-to-Cloud
      - Backend Data Sharing
  - Layers
    - Edge Technology
      - Sensors
      - Devices
    - Access Gateway
      - First Data Handling Layer
    - Internet
    - Middleware
      - Between Application and Hardware
    - Application
      - Deliver Services and Data to Users
- Vulnerabilities and Attacks
  - Tools
    - Censys
    - Shodan
    - IoT Sploit
    - Thingful
    - Tenable IoT
    - IoT Inspector
    - Firmalyzer
    - Killer Bee
    - Foren6
    - JTAGulator
    - CloudShark
  - Countermeasures
    - Hardening
    - Remove Unused Accounts & Services
    - Implement IDS
    - Lockout Features
    - Secure Communication (VPN)
    - Monitor Ports
    - DMZ Zones
- Hacking Methodology
  - Info Gathering
  - Vuln Scanning
  - Launch Attacks
  - Gain Access
  - Maintain Access

Mobile Attack Surface

- The Device Itself
  - Browser Attacks
  - SMS Attacks
  - Applications Attacks
  - Rooting & Jailbreaking
  - BYOD Policy
  - MDM Systems
- Network Attacks
  - DNS Cache Poison
  - Rogue Access Points
  - Packet Sniffing
  - Vectors
    - 4G, 5G, etc
    - Bluetooth
- Cloud Attacks
  - External Resources
  - Databases

Rooting & Jailbreaking

- Android
  - Kingo Root
  - OneClickRoot
  - MTK Droid
- iOS
  - Cydia
  - Hexxa Plus
  - Apricot
  - yuxigon
  - Techniques
    - Untethered JB — Kernel Remains Patched After Reboot
    - Semi-tethered JB — Reboot Doesnt Retain Patched Kernel
    - Tethered JB — Reboot Removes Jailbreaking Patches
  - Types
    - Userland Exploit — User-level Access
    - iBoot Exploit
      - Found in Device Bootloader
      - Turn Codesign Off
      - Admin Access
    - BootROM Exploit
      - Access to Filesystem, SecureROM
      - Hardware
      - Admin Access

OWASP Top 10

- Mobile
  - M1: Improper Platform Usage
  - M2: Insecure Data Storage
  - M3: Insecure Communication
  - M4: Insecure Authentication
  - M5: Insufficient Cryptography
  - M6: Insecure Authorization
  - M7: Client Code Quality
  - M8: Code Tampering
  - M9: Reverse Engineering
  - M10: Extraneous Functionality
- IoT
  - I1: Weak, Guessable, or Hardcoded Passwords
  - I2: Insecure Network Services
  - I3: Insecure Ecosystem Interfaces
  - I4: Lack of Secure Update Mechanism
  - I5: Use of Insecure or Outdated Components
  - I6: Insufficient Privacy Protection
  - I7: Insecure Data Transfer and Storage
  - I8: Lack of Device Management
  - I9: Insecure Default Settings
  - I10: Lack of Physical Hardening

Mobile Attacks

- Phishing — Smishing
- Social Engineering
- Mobile Device Management Tools
  - Android Lost
  - Find My Phone
- Bluetooth
  - Bluesmacking — DoS
  - Bluejacking — Unsolicited Messages
  - Bluesniffing — Discover BT Devices
  - Bluebugging — Remote Access
  - Bluesnarfing — Theft of Data Via Open Connection
  - Blueprinting — Footprinting Bluetooth Devices
  - Modes
    - Discovery Mode
      - Discoverable Action
      - Limited Discoverable Action
      - Non Discoverable
    - Pairing Mode
      - Yes (Pairable)
      - No (Nonpairable)
  - Tools
    - Bluescanner
    - BT Browser
    - BlueSniff
    - BT Crawler
    - Bloover
    - Super Bluetooth Hack

XMind Evaluation Mode