SEC617.1: Wi-Fi Data Collection and Analysis

Characterize the Wireless Threat

- Recognizing protocol weaknesses and cryptographic failures across wireless technologies
- Why popular smart phones increase our exposure to attack
- Anatomy of a wireless attack: How real-world attackers exploit wireless systems
- Introduction to the SWAT kit

Sniffing Wi-Fi

- Leveraging built-in functionality in every Wi-Fi card for penetration testing
- Wireless packet capture on Linux, Windows, and macOS
- Overcoming physical-layer challenges in IEEE 802.11n, IEEE 802.11ac packet sniffers
- Detecting cheaters: Radio regulatory domain bypass hacks
- Packet capture, filter, and analysis with tcpdump, Wireshark, and Kismet
- Tools and techniques for understanding your radio frequency exposure with topographic range mapsRogue Access Point (AP) Analysis
- Characterizing the threat and attacker motives for rogue APs
- Wired-side analysis for rogue APs using open-source tools
- Filtering out Wi-Fi noise to focus on and characterize rogue device threats
- Correlating Wi-Fi devices with your network infrastructure
- Effective unauthorized transmitter location analysis techniques

SEC617.2: Wi-Fi Attack and Exploitation Techniques

Exploiting Wi-Fi Hotspots

- Bypassing authentication on hotspot networks
- Exploiting mobile application data disclosure on open networks
- Luring Wi-Fi client victims with Wi-Fi hotspot impersonation
- Leveraging sidejacking attacks against hotspot networks

Wi-Fi Client Attacks

- Leveraging Wi-Fi timing attacks for traffic manipulation
- Bypassing client isolation security on Wi-Fi networks
- Wi-Fi client privacy and isolation attacks through preferred network list disclosure
- Leveraging commercial tools such as the Wi-Fi Pineapple for AP impersonation
- Integrating Metasploit Meterpreter payloads in Wi-Fi network injection attacks

Exploiting WEP

- A brief look at WEP technology and exploitation
- Applying the cryptography in WEP to non-Wi-Fi protocols

Denial of Service (DoS) Attacks

- Identifying types of DoS attacks and attack targets
- Leveraging RF jammers in a pen test
- Selective client DoS targeting to manipulate network roaming events
- Single-client to entire-network Wi-Fi DoS techniques

Wi-Fi Fuzzing for Bug Discovery

- Introduction to fuzzing techniques
- Identifying complex parsing issues in Wi-Fi protocols
- Using Scapy to build malformed packets
- Identifying bugs in APs and client devices through fuzzing
- Applying fuzzing as part of an overall Wi-Fi security analysis

SEC617.3: Enterprise Wi-Fi, DECT, and Zigbee Attacks

Attacking WPA2 Pre-Shared Key Networks

- In-depth analysis of key derivation functions in WPA2
- Capturing and evaluating WPA2-PSK client network authentication exchanges
- Attacking the passphrase selection of WPA2-PSK

Attacking WPA2 Enterprise Networks

- Differentiating PSK-based WPA2 and WPA2 Enterprise networks
- Leveraging identity disclosure in WPA2 Enterprise networks
- Exploiting Windows 10 Native Wi-Fi and PEAP networks
- Exploiting iOS and Android Enterprise Wi-Fi network roaming behavior
- Using Hostapd-WPE for Enterprise network impersonation
- Password recovery through MS-CHAPv2 cracking

Attacking Digital Enhanced Cordless Telephony Deployments

- DECT as a cordless telephony and data application technology
- DECT physical and MAC layer fundamentals
- Evaluating the DECT authentication and encryption mechanisms
- Eavesdropping and recording audio conversations on DECT cordless phones

Attacking Zigbee Deployments

- In-depth analysis of Zigbee and IEEE 802.15.4 physical and MAC layer architecture
- Zigbee and IEEE 802.15.4 authentication and cryptographic controls
- Weaknesses in Zigbee key provisioning and management mechanisms
- Tools for eavesdropping on and manipulating Zigbee networks
- Exploiting Zigbee Over-the-Air key provisioning
- Locating Zigbee devices with signal analysis tools

SEC617.4: Bluetooth and Software Defined Radio Attacks

Bluetooth Introduction and Attack Techniques

- Understanding the physical layer evolution of Bluetooth and packet capture techniques
- Bluetooth pairing techniques and vulnerabilities
- Attacking Bluetooth pairing for PIN and key recovery
- Techniques for identifying non-discoverable Bluetooth devices

Bluetooth Low Energy Introduction and Attack Techniques

- Recognizing BLE Frequency-Hopping RF patterns
- Security analysis of BLE pairing options -- just works, OOP, passkey, and numeric comparison
- Analysis of expensive and inexpensive BLE packet capture tools for Windows, Linux, and Android devices
- Scanning BLE device services with bluetoothctl, Android apps, and related tools
- Practical exploitation of BLE services

Practical Application of Software-Defined Radio (SDR)

- Guide to using SDR in a penetration test
- RF spectrum visualization and signal hunting with SDR# and GQRX
- Decoding ADS-B aircraft beacon traffic
- Eavesdropping on POCSAG and FLEX pager messaging
- GSM cell tower scanning and evaluation with SDR
- Leveraging capture and replay attacks to exploit vehicle keyless entry systems

SEC617.5: RFID, Smart Cards, and NFC Hacking

RFID Overview

- Understanding the components, transmission frequencies, and protocols in RFID systems
- Differentiating active and passive RFID systems
- Understanding NFC systems components and protocols
- Practical range extensions in RFID attacks

RFID Tracking and Privacy Attacks

- Practical location disclosure attacks in RFID systems
- Case study: E-Z Pass location disclosure threats
- Manipulating Apple iBeacon location tracking systems
- RFID tracking through Ultra-High Frequency (UHF) tags

Low-Frequency RFID Attacks

- Case study: cloning RFID tags used for bike rental systems
- Leveraging RFIDiot for low-frequency RFID attacks
- Attacking HID ProxCard proximity lock systems
- Leveraging the ProxMark RDV2 for low-frequency RFID attacks
- Brute-forcing HID identifiers for unauthorized access
- Extending range in HID cloning attacks
- Manual low-frequency tag analysis and bitstream decoding

Exploiting Contactless RFID Smart Cards

- Conducting smart card reconnaissance analysis with Linux and Android
- Attacking Europay-Mastercard-Visa (EMV) PoS systems
- Exploiting MIFARE Classic smart card systems
- Effective smart card cloning with UID impersonation
- Attacking MIFARE Ultralight, Ultralight-C, and DESFire smart card systems
- Emulating smart cards with the ProxMark RDV2

Attacking NFC

- Decoding the NFC Data Exchange Format (NDEF) protocol
- Reading and writing NFC/NDEF tags
- Analysis of Android Beam, Google Wallet, and Apple Pay NFC systems
- Exploiting NFC smart toys
- Attacking Android devices with malicious NFC tags

SEC617.6: Hands-on Capture-the-Flag Event