Course ID
WIFI-NOS
Course Duration
4 days

Course Title

Wi-Fi Local Area Network Operation and Security

Related Courses

- WIFI: A Tutorial for Those Familiar with Wireless/Cellular Networks (WIFI-TO, 3 days)
- Wi-Fi Technology: Principles and Operation (WIFI, 3 days)
- Metropolitan WiFi Network Design and Deployment (WIFINET, 4 days)
- IEEE 802.11 (WiFi) Wireless LAN Security (WIFISEC, 3 days)
- Wi-Fi: Technology, Applications, Design, and Deployment (WIFI-TECH, 2 days)
- State-of-the-art of WiFi for Non-engineering Professionals, Managers, and Executives (WIFI, 1 day)

Aimed At

Technical personnel interested in Wi-Fi LAN technology, network operation, and network security.

Group Size

5-25

Prerequisites

Those wishing to take this course should have background in telecommunications or IT with a basic understanding of data networks.

Course in a Nutshell

This course is aimed at those interested in learning WiFi architecture and operation with particular interest in the security issues, such as those involved in performing security audits of WiFi networks. However, with content adjustment as needed, the course will benefit other audiences as well.

Customize It!

Let us know your reason for studying WiFi so we can tailor the course accordingly. The standard course is four days long but can be shortened or expanded as required.

Course Outline

Part 1: Introduction to IEEE 802.11 and Wi-Fi

- Wired vs wireless communications
  - Comparison of security challenges
- Introduction to security attacks and countermeasures
  - Layered security attack methods
  - Shared key and public key cryptography
- Overview of IEEE 802.11 and Wi-Fi
  - General architecture
  - Wi-Fi Alliance
  - IEEE 802.11 task groups

Part 2: Wi-Fi Physical (PHY) Layer

- Range calculations and PHY vulnerabilities
  - Calculating maximum range
  - Eavesdropping range of vulnerability
  - Jamming range of susceptibility
  - Countermeasures
- Basic modulation methods
  - Modulated signal structure
  - Amplitude, frequency, and phase shift keying
- Direct sequence spread spectrum (802.11b)
  - DSSS methods
  - Processing gain
  - Complementary code keying (CCK)
- Advanced modulation methods (802.11g/n)
  - Quadrature Amplitude Modulation (QAM)
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - Performance
- Advanced antennas and multiple-input multiple-output (MIMO)
  - 802.11n MIMO
  - 802.11n operating modes and performance
- Error Control
  - Error detection and correction
  - Automatic repeat request

Part 3: Wi-Fi Medium Access Control (MAC)

- Carrier-sense multiple access
  - Basic concept and operation
  - Avoiding network instability

    - CSMA and denial-of-service (DoS) attacks
- Distributed Coordination Function (DCF)
    - Channel access and backoff
    - Performance
    - DCF and man-in-the-middle (MITM) attacks
- Point Coordination Function (PCF)
    - Channel access and scheduling
    - Performance
- Quality-of-Service
    - The QoS challenge
    - Overview of 802.11e QoS enhancements
- Throughput capabilities
    - Frame transmission times
    - Throughput analysis
- Management operations
    - Connection process
    - Addressing and traffic flow

Part 4: IEEE 802.11i Access Control and Key Management

- Introduction to Robust Security Network (RSN)
    - RSN security layers
    - Methods of authentication
    - 802.11i operational phases
- 802.1X Port-Based Network Access Control
    - 802.1X authentication and key distribution
    - Digital certificate
    - Challenge-response using a RADIUS server
- Extensible Authentication Protocol (EAP)
    - EAP request/response
    - EAP over LAN (EAPOL)
    - Key derivation and exchange
- Transport Layer Security (TLS)
    - TLS handshake exchange
    - TLS and 802.11i
    - TLS over EAP
- Security while roaming
    - Preauthentication

Part 5: IEEE 802.11i Encryption

- Wired Equivalent Privacy (WEP) weaknesses
  - Desired security criteria
  - WEP operation
  - Weaknesses: Authentication, data confidentiality, data integrity
- Temporal Key Integrity Protocol (TKIP)
  - TKIP implementation
  - Encapsulation and decapsulation processes
  - TKIP message integrity
  - TKIP attack countermeasures
- Advanced Encryption Standard (AES)
  - Requirements for WEP replacement
  - AES operation
  - AES modes and algorithms
  - 802.11i counter/cipher block chaining with message authentication code (CCM) protocol

Part 6: Wi-Fi Protected Access (WPA)

- IEEE 802.11i and Wi-Fi Protected Access (WPA)
  - Comparison of 802.11i and WPA
- Versions of WPA
  - WPA Personal vs WPA Enterprise
  - WPA vs WPA2
- WPA and RSN key hierarchy
  - Pairwise and group keys
  - Key hierarchy
  - Key derivation
- WPA implementation requirements
  - Access points
  - Network adaptors
  - Client software
- WPA certification

Part 7: Wi-Fi Network Attack and Defense Methods

- Specific attack methods
  - Planning and executing an attack
  - Summary of specific attack methods
- General methods for enhancing Wi-Fi security
  - AP placement
  - AP setup
  - Security outside of WPA/802.11i

- Network analysis tools
  - Spectrum analyzer
  - Protocol analyzer
  - Other analyzers
- Wireless Intrusion Detection Systems (WIDS)
  - Intrusion detection
  - Intrusion prevention
  - Implementation
  - Survey of available WIDS products
- Wrap-up
  - Course Recap and Q/A
  - Evaluations

How You Will Learn

- A seasoned instructor well versed in WiFi and other wireless technologies will present this course in interactive lecture format.
- Along with the lecture, we will use exercises to enrich the instruction and drive home the essential points.
- If you already know something about the technology, we will build on that. We'll compare and contrast what's familiar with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *June 22, 2011f*