

Course ID

**WIFISEC**

Course Duration

**3 days**

**Aimed At**

Course Title

**IEEE 802.11 (WiFi) Wireless LAN Security**

Engineers, product developers, managers, security officers, city/state government or law enforcement professionals, wireless Internet service providers, and network administrators who have a special concern for wireless security and are interested in evaluating, designing, or implementing 802.11 wireless local area networks.

**Group Size**

5-25

**Course**

**In a Nutshell**

In this three-day course, you will undertake an in-depth study of the IEEE 802.11 (WiFi) wireless local area network security issues.

Aspects of disclosure, data integrity, and denial-of-service threats are reviewed. Principles of indoor RF propagation are used to calculate the extent of eavesdropping and jamming threats to the physical layer. The 802.11 Medium Access Control (MAC) methods are looked at and the numerous threats to this layer are discussed. Next, Wired Equivalent Privacy (WEP) is presented and its weaknesses examined in areas of disclosure, data integrity, and authentication. The IEEE 802.11i-based solutions are discussed, beginning with interim solutions such as Temporal Key Integrity Protocol (TKIP), and moving on to stronger solutions based on the Advanced Encryption Standard (AES). The synergies between Wi-Fi protected access (WPA) and 802.11i are explored. Finally, upper layer authentication and key management as provided by IEEE 802.1X are discussed.

**Customize It!**

We can customize this course to the requirements of particular audience groups to make the course more or less technical or to focus on the specific issues of interest to them. We perform most tailoring at little to no additional cost.

**Learn How To**

- Describe general security threats on disclosure, data integrity, and denial-of-service
- Calculate the extent of security vulnerabilities at the physical layer
- Describe various security threats at the IEEE 802.11 Medium Access Control (MAC) layer
- Demonstrate an in-depth understanding of Wired Equivalent Privacy (WEP) operation and weaknesses
- Comprehend IEEE 802.11i robust security network (RSN) operations
- Describe the operation of temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES)
- Demonstrate 802.1X authentication and key management operation
- Show how the various WEP vulnerabilities are addressed by RSN

**Course  
Outline**

*Day One*

- Introduction
  - Security overview
  - Short-range wireless systems
  - WLAN characteristics
  - Categories of information transmission
  - Security threats
  - IEEE 802.11 operations overview
- Propagation and Range Limit
  - Review of decibels
  - Link budget equation and path loss model
  - Calculating maximum range
  - Partition attenuation and primary ray tracing
  - Eavesdropping and jamming vulnerabilities
  - Multipath characteristics and mitigation
- 802.11 Physical Link
  - RF modulation methods used in 802.11 a/b/g
  - Direct sequence spread spectrum
  - Operating frequencies and signal spectrum
  - 802.11b radio requirements
  - Modeling interference and jamming

*Day Two*

- 802.11 Physical Link (continued)
  - 802.11b PHY packet structure
  - Orthogonal Frequency Division Multiplexing (OFDM)
  - 802.11a/g radio requirements
  - 802.11a/g jamming vulnerability
  - 802.11a/g PHY packet structure
  - Multiple-Input Multiple-Output (MIMO) methods
- 802.11 Medium Access Control (MAC)
  - Carrier-sense multiple-access operation and throughput
  - Distributed coordination function (DCF) operation
  - Point coordination function (PCF) operation
  - MAC frame construction and examples
  - IEEE 802.11e quality-of-service (QoS) operation
  - 802.11 management operations

### *Day Three*

- Wired Equivalent Privacy (WEP)
  - Shared key and public key cryptography
  - Cryptanalysis attack methods
  - WEP encryption process and weaknesses
  - WEP data integrity process and weaknesses
  - WEP access control process and weaknesses
  - Denial-of-service attack methods
  - Bluetooth security overview and comparison to WEP
- Security Enhancements
  - IEEE 802.11i robust security network (RSN) overview
  - Temporal Key Integrity Protocol (TKIP) operation and vulnerability
  - Advanced Encryption Standard (AES) operation and implementation
  - AES counter mode with cipher block chaining protocol (CCMP) operation
  - 802.1X extensible authentication protocol (EAP) and variants
  - 802.1X key distribution methods
  - RSN information elements
  - Wi-Fi Protected Access (WPA) operation
  - Security analysis and cracking tools
  - Virtual Private Network (VPN) operation
- Wrap-Up: Course Recap, Q/A, and Evaluations

### **How You Will Learn**

- An experienced engineer-instructor who is well-versed in wireless network security and a variety of short-range wireless technologies will teach this course.
- The course will be presented as a hands-on tutorial with discussion, exercises, and interesting activities interspersed throughout the class.
- The instructor will use real-life examples, applications, and exercises to make the class more practical.
- You will receive a participant handbook designed to provide a record of the class presentation as well as your own notes and insights for later recall and use.

*Revised*

*April 20, 2008f*