

Wireless LAN Security Course Outline 3.0

The Wireless LAN Security 3.0 course, whether in an academic format or a 5-day fast-track format, provides the wireless security professional a complete foundation of knowledge for entering into or advancing in the wireless security industry. From small/medium business (SMB) to enterprise-class wireless security, this course delivers hands-on training that will benefit the administrator as well as the security consultant.

- Audience:** Administrators, Consultants, and Architects
Duration: 5 days, Classroom. May be taught over 1 academic semester.
Associated Certification: CWSP
Prerequisites: Basic networking knowledge (OSI / IP). Basic network security concepts, and wireless network administration knowledge.

Introduction to WLAN Security Technology

- Security policy
- Security concerns
- Security auditing practices
- Application layer vulnerabilities and analysis
- Data Link layer vulnerabilities and analysis
- Physical layer vulnerabilities and analysis
- 802.11 security mechanisms
- Wi-Fi Alliance security certifications

Small Office / Home Office WLAN Security Technology and Solutions

- WLAN discovery equipment and utilities.
- Legacy WLAN security methods, mechanisms, and exploits
- Appropriate SOHO security

WLAN Mobile Endpoint Security Solutions

- Personal-class mobile endpoint security
- Enterprise-class mobile endpoint security
- User-accessible and restricted endpoint policies
- VPN technology overview

Branch Office / Remote Office WLAN Security Technology and Solutions

- General vulnerabilities
- Preshared Key security with RSN cipher suites
- Passphrase vulnerabilities
- Passphrase entropy and hacking tools
- WPA/WPA2 Personal – how it works
- WPA/WPA2 Personal - configuration
- Wi-Fi Protected Setup (WPS)
- Installation and configuration of WIPS, WNMS, and WLAN controllers to extend enterprise security policy to remote and branch offices

Enterprise WLAN Management and Monitoring

- Device identification and tracking
- Rogue device mitigation
- WLAN forensics
- Enterprise WIPS installation and configuration
- Distributed protocol analysis
- WNMS security features
- WLAN controller security feature sets

Enterprise WLAN Security Technology and Solutions

- Robust Security Networks (RSN)
- WPA/WPA2 Enterprise – how it works
- WPA/WPA2 Enterprise - configuration
- IEEE 802.11 Authentication and Key Management (AKM)
- 802.11 cipher suites
- Use and design of authentication services (RADIUS, LDAP) in WLANs
- User profile management (RBAC)
- Public Key Infrastructures (PKI) used with WLANs
- Certificate Authorities and x.509 digital certificates
- RADIUS installation and configuration
- 802.1X/EAP authentication mechanisms
- 802.1X/EAP types and differences
- 802.11 handshakes
- Fast BSS Transition (FT) technologies

Hands-on Lab Exercises

WLAN Controller Security

The WLAN controller is currently the center piece of 802.11 security. All other pieces of the WLAN security puzzle orbit around the WLAN controller. For this reason, gaining an in-depth understanding of how to secure access to the controller and how to use the controller to secure the WLAN is essential.

This lab is focused on WLAN controller security, and primarily covers the following areas:

1. Secure access to the WLAN controller using secure management protocols.
2. Configuring multiple WLAN profiles, each with its own authentication and cipher suites including WPA/WPA2 Personal and Enterprise.
3. Configuring the WLAN controller for RADIUS connectivity and authentication.
4. Client station connectivity to the controller – including DHCP and browsing.
5. Integrated rogue device discovery.

Wireless Intrusion Prevention Systems (WIPS)

This lab is focused on Wireless Intrusion Prevention Systems (WIPS). WIPS are known for three overriding functions: security monitoring, performance monitoring, and reporting. In this lab exercise, we will focus only on security monitoring and reporting. Areas of particular interest include:

1. WIPS installation, licensing, adding/configuring sensors, and secure console connectivity.
2. Configuration according to organizational policy.
3. Properly classifying authorized, unauthorized, and external/interfering access points.
4. Identifying and mitigating rogue devices.
5. Identifying specific attacks against the authorized WLAN infrastructure or client stations.

Using Laptop Analyzers

This lab is focused on the use of laptop analyzers for spectrum analysis, protocol analysis, and WLAN discovery. Understanding driver issues, security-related protocol analysis (authentication and encryption), and spectrum analysis will aid the wireless security professional in policy compliance, proper implementation, and troubleshooting. The following steps will be covered in this lab exercise.

1. Installing and configuring a WLAN discovery tool.
2. Installing, licensing, and configuring a laptop protocol analyzer.
3. Installing, licensing, and configuring a laptop spectrum analyzer.
4. Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN discovery tool.
5. Locating and analyzing 2.4 GHz and 5 GHz WLANs with a WLAN protocol analyzer.
6. Capturing and analyzing a WPA2-Personal authentication in a WLAN protocol analyzer.
7. Capturing and analyzing a WPA2-Enterprise authentication in a WLAN protocol analyzer.
8. Capturing and analyzing Hotspot authentication and data traffic in a WLAN protocol analyzer.

9. Capturing and analyzing Beacons, Probe Requests, Probe Responses, and Association Requests with a WLAN protocol analyzer.
10. Viewing a normal RF environment, a busy RF environment, and an RF attack on the WLAN in a spectrum analyzer.

Fast BSS Transitions (FT)

This lab is focused on fast BSS transition (FT) within an Extended Service Set. Moving quickly and securely between access points attached to a single controller or multiple controllers is a requirement of real-time mobility devices such as wVoIP phones and mobile video devices. An in-depth understanding of the standards-based and proprietary processes of a WLAN infrastructure system's ability to deliver FT services means the difference between a successful deployment and a complete failure. The following steps will be covered in this lab exercise.

1. Configure a WLAN infrastructure with two controllers and two APs per controller. Configure APs for specific power and channel settings.
2. Install and configure a RADIUS server for PEAP.
3. Configure both controllers and an authorized client device for PEAP authentication using the CCMP cipher suite.
4. Configure an 802.11 protocol analyzer to capture on a specific channel.
5. Using an 802.11 frame generator function, deauthenticate the authorized client station to force intra- and inter-controller roaming.
6. Perform a slow BSS transition within a controller as a baseline.
7. Enable FT mechanisms within controllers and the client station.
8. Perform a fast BSS transition within a controller as a comparison.
9. Perform a slow BSS transition between controllers as a baseline.
10. Perform a fast BSS transition (if vendor FT mechanisms permit) between controllers as a comparison.

