

# WIRELESS LAN Security Workshop (WL-SEC, 3 days)

## Course Description

This course teaches the essential WLAN Security concepts and protocols from technical and design perspectives. You will learn WLAN transmission protocols and frame formats to understand the root of WLAN vulnerabilities, and how to apply that knowledge to WLAN security design, monitoring and response concepts.

This course is highly interactive with hands-on exercises covering design, build, scanning, penetration and vulnerability testing aspects.



## Who Can Benefit

- Network and Systems Administrators
- LAN Designers and Infrastructure Integrators and Consultants
- Network, Infrastructure and general IT managers
- IT Security staff at all levels

## Prerequisites

**To succeed fully in this course, participants should have:**

- WLAN foundation
- Or attended WLAN Fundamentals

## Skills Gained

**Upon completion of this course, participants should understand:**

- Wireless security standards, including WEP, WPA, WPA2 and 802.11i
- WLAN Security Design principles
- Wired Equivalent Privacy (WEP) protocols and inherent limitations
- WPA protocols and how they address some of the limitations of WEP
- WPA2 protocols and configuration best practices
- WLAN Authentication methods and selection
- 802.1X/EAP methods and selection
- Methods for preventing, detecting, responding to, and auditing state-of-the-art WLAN attacks
- The critical role of Wireless intrusion detection for maintaining a secure network

---

### REGISTRATION AND INFORMATION

[education@ecs.com.sg](mailto:education@ecs.com.sg)  
[www.ecs.com.sg/training](http://www.ecs.com.sg/training)

# WIRELESS LAN Security Workshop (WL-SEC, 3 days)

## Course Content

### Module 1 - WLAN Security Infrastructure

- Basic enterprise WLAN architecture
- WPA2 Enterprise
- Station protection
- Data protection
- Network protection
- Access points
- Controllers
- WNMS
- RADIUS servers
- Wireless VLANs

### Module 2 - 802.11 Security (WEP)

- WEP authentication options
- Open system
- Shared key
- WEP encryption
- Key management
- WEP integrity
- WEP flaws

### Module 3 - RSN Authentication

- PSK authentication
- PSK cracking
- 802.1X/EAP authentication
- 802.1X/EAP design
- 802.1X/EAP cracking
- EAP type selection

### Module 4 - RSN Encryption

- Fixing and replacing WEP
- TKIP encryption
- AES-CCMP encryption
- AES-CCMP protocols
- AES-CCMP design
- Data frame encryption
- Frame encapsulation

### Module 5 - RSN Key Management

- Fast transition
- PMK caching
- RSN key material
- Unicast encryption
- Broadcast/multicast encryption
- Pairwise transient key structure
- 4-way handshake
- Group key handshake
- Peer key handshake

### Module 6 - Network Security

- Prevention
- Unauthorized access
- Authentication options
- MAC address spoofing
- Network segmentation
- Rogue APs
- Rogue AP detection and response
- Denial of service detection and response
- RF jamming detection and response
- Auditing and Monitoring
- Wireless IDS/IPS
- WNMS

### Module 7 - Wireless Data Security

- Wireless traffic security
- Eavesdropping
- Encryption options
- Internal encryption: WPA2
- External encryption: VPNs
- Endpoint security
- ESS
- NAC
- Auditing
- Wireless IDS/IPS
- Protocol analyzers

---

## REGISTRATION AND INFORMATION

[education@ecs.com.sg](mailto:education@ecs.com.sg)  
[www.ecs.com.sg/training](http://www.ecs.com.sg/training)

