

Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA/CWSP, CPTS/CPTE  
Principal Consultant, WaveFront Consulting Group  
[ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) | 1 (604) 961-0701 | [www.wavefrontcg.com](http://www.wavefrontcg.com)

## Introduction

Insecure wireless networks at two discount stores in Miami FL allowed attackers to gain a beachhead in TJMaxx's (TJX) computer network in July 2005. Instead of the more secure WPA technology, these two stores were still using WEP encryption. Information on over 45.7M credit and debit cards was stolen over several years, in addition to private information such as driver's license and social insurance numbers. This information was used for a fraudulent gift card scheme (\$8M), identity theft, credit card fraud (\$68M for Visa), etc. The costs to TJMaxx are so far pegged at over \$150M US. This breach occurred because of an insecure wireless network configuration, and practices which were in violation of Canadian privacy laws, US data breach laws, and the Payment Card Industry's Data Security Standard (PCI DSS). See [http://www.boston.com/business/technology/articles/2008/08/17/the\\_breach](http://www.boston.com/business/technology/articles/2008/08/17/the_breach) for more information.

Wireless signals are not constrained by wires like the electrical signals used in traditional networks. Wireless signals travel everywhere and can be easily captured by someone in the parking lot, in the next building, or across the river. Unless wireless signals are strongly encrypted to prevent eavesdropping, and controls put in place to ensure only authorized users are allowed to connect, wireless networks provide hackers and cyber-criminals with an easy backdoor into corporate networks, as TJMaxx and many others have found to their embarrassment and financial loss.

## Course Description

This four day hands-on course is intended to provide network and system administrators with the knowledge and skills necessary to securely design, deploy and manage enterprise-wide wireless local area networks; and to test the security of wireless networks for weaknesses. Students are trained to setup wireless networks to increasing levels of security, and shown how the weaknesses of various wireless technologies can be exploited to gain unauthorized access. Network and Security Architects, IT Security practitioners, auditors and compliance officers (especially those involved with PCI DSS compliance) would also benefit from this training.

## Learning Outcomes

At the end of this course the student should be able to:

- Understand local area wireless network technologies (802.11, Bluetooth, RFID), and their security weaknesses;
- Architect a secure wireless network infrastructure for their organization, including strong encryption and centralized authentication;
- Understand the hacker threat and the major techniques hackers use against wireless networks;
- Use various hacking and vulnerability assessment tools to assess the security of wireless networks, including cracking WEP and WPA security;
- Identify (and fix) vulnerabilities and mis-configurations in wireless network technologies;

This is a hands-on course, with a mix of lectures, demonstrations, labs and exercises.

## Pre-Requisites

The course is intended for security professionals, auditors, and system and network administrators. A good technical understanding of computer systems (primarily MS Windows) and networks (TCP/IP) is a pre-requisite for taking this course. UNIX/Linux experience is not necessary. However, since many wireless security tools are Linux based, students will be given some background training on this environment. A brief overview of local wireless network technologies (802.11 and Bluetooth) is also provided.

All equipment (incl. wireless access points, network cards and antennas), as well as software, is provided.

## Our Trainer

This course was developed and is presented by our Chief Trainer, Mr. Rui Pereira, B.Sc.(Hons), CIPS, CISSP, CISA, CWNA/CWSP, CPTS/CPTE. Rui has over 25 years of experience in the IT industry, the last 13 in Information Security and Audit (with several wireless network deployments and many penetration tests under his belt). Rui is a Certified Wireless Network Administrator (CWNA) and Certified Wireless Security Professional (CWSP). In addition to WaveFront's suite of IT Security courses, Rui has also developed and teaches several courses at the University of British Columbia (UBC) and the British Columbia Institute of Technology (BCIT). Rui's biography and resume are available online at [www.wavefrontcg.com/PrincipalConsultants.html](http://www.wavefrontcg.com/PrincipalConsultants.html).

## Course Outline

### Day 1 - **Introductions to Wireless Networking, Lab Environment, Cryptography for Wireless Networks**

#### **Introduction**

- The Threat Landscape
- Wireless Insecurity
- Wireless Network Attacks
  - Passive vs. Active Attacks
  - Man-in-the-Middle Attacks
  - Rogue Access Points and Client Attacks
  - Denial of Service (DoS) Attacks
- The Law
  - FCC and Industry Canada
  - US and Canadian Legislation
  - PCI DSS Requirements
- Further Training and Certifications
  - CWNA and CWSP Certifications

#### **Introduction to Wireless Networking**

- Wireless LAN Applications
- Wireless LAN Organizations
  - IEEE, IETF and Wi-Fi Alliance
- 802.11 Wireless LAN Standards
  - 802.11a/b/g/n
- Bluetooth and Other Wireless Technologies

- Wireless LAN Basics
  - Radio Frequency Fundamentals
  - Spread Spectrum (FHSS, DSSS, OFDM)
  - Interference and Throughput
- Wireless Equipment
  - Access Points and Wireless Clients
  - Ad-hoc vs. Infrastructure Networks
  - Service Sets
  - Wireless LAN Management
  - Wireless Gateways, Bridges and Switches
  - Antennas
- Spectrum Usage
  - Channels
  - ISM and UNII Bands

### **The Lab Environment**

- Your Workstation
- Wireless Equipment
- Virtual Machines
- Windows and Linux Tools
- Lab #1 - Wireless Setup
- Lab #2 – Using and Breaking MAC Address Filters
- Lab #3 – Eavesdropping on Wireless networks

### **Cryptography for Wireless Networks**

- Conceptual Foundation
- Symmetric Cryptography
  - Block and Stream Ciphers
  - Cipher Modes
  - Authentication and Integrity
  - Message Authentication Codes (MAC's)
- Asymmetric Cryptography
  - Encryption and Signing
  - Hashes and Message Digests
  - Public Key Infrastructure (PKI)
- Hybrid Cryptography
- Cryptography for Network Traffic
  - SSL, IPSec and SSH
- Key Management
- Attacking Crypto
  - Cryptographic and non-Cryptographic Attacks
  - Key Lengths

Day 2 - **Security Concepts, WLAN Discovery, Authentication, Confidentiality & Integrity**

**Security Concepts**

CIA & AAA  
Vulnerabilities, Threats, Exploits, Risks and Controls  
Wireless Security

**Wireless LAN Discovery**

Passive and Active Scanning  
    Authentication and Association  
Discovery and Mapping Tools  
    Windows and Linux Tools  
    NetStumbler and Inssider (Demos)  
    Kismet (Demo)  
Lab #4 - WLAN Discovery (Netstumbler, Kismet)  
War Driving and Chalking  
    Equipment (Antennas, GPS)  
    Mapping Software (Stumbverter, JiGLE, MapPoint, Google Earth)  
Wireless Network Sniffing  
    WireShark and AeroPeek (Demos)  
Exercise #1 – Wireless Protocol Analysis  
Spectrum Analyzers

**Wireless LAN Authentication**

WEP for Authentication  
    Open vs. Shared Key  
802.1X  
    Supplicants and Servers  
Extensible Authentication Protocols  
    EAP Authentication Types  
    LEAP and PEAP  
WPA Authentication  
    WPA-PSK  
Lab #5 - WPA-PSK Setup  
Hacking WPA-PSK  
    Aircrack-ng and coWPATy (Demos)  
Lab #6 - Hacking WPA-PSK (aircrack-ng)  
LEAP and PEAP  
    Hacking LEAP with asLEAP (Demo)  
Lab #7 - WPA Enterprise Setup (PEAP)

## **Wireless LAN Confidentiality & Integrity**

- Wired Equivalent Privacy (WEP)
  - How WEP Works
  - WEP Cryptographic Weaknesses
  - Other Problems with WEP
- Lab #8 - WEP Setup
- Hacking WEP
  - Aircrack-ng (Demo)
  - Other WEP Cracking Tools (AirSnort, WEPAAttack)
- Lab #9 - Hacking WEP (aircrack-ng)
- Fixing WEP
  - TKIP and MIC
  - WPA1, WPA2, WPA-PSK
- 802.11i and the 4-Way handshake
  - Distributing Keys

Day 3 - **More WLAN Security, Bluetooth Security, Wireless Security Guidelines**

### **More Wireless LAN Security**

- SSID, Protocol and MAC Address Filtering
- Virtual LAN's (VLAN's) and Network Segmentation
  - AP Isolation and Guest Networks
- Securing the Upper Layers
  - Virtual Private Networks (VPN's)
  - Other Network Protocols (SSL, SSH, SNMP)
  - Management Interfaces
  - Firewalls and DMZ's
- Lab #10 - Other Wireless Security Setup
- Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS)
  - Kismet, AirDefense
  - Kismet IDS (Demo)
  - Rogue AP Detection
  - Intrusion Forensics
- Lab #11 – Configuring WIDS (Kismet)
- WLAN Management
  - WLAN Controllers
  - WLAN Management Software
  - Captive Portals
- Protocol and Spectrum Analyzers
  - AirMagnet and Wi-Spy (Demos)

## **Bluetooth Security**

- BlueTooth Background and Usage
- BlueTooth Security Controls and Weaknesses
- Hacking BlueTooth
  - BlueSnarfing, BlueBugging and BlueJacking
  - BlueTooth Hacking Tools
  - BTScanner (Demo)

## **Wireless Security Guidelines**

- Policies, Procedures and Guidelines
- Wireless Security Architecture and Baseline Practices
- Authentication - WEP, WPA-PSK, WPA-Enterprise
- Confidentiality - WEP, WPA, TKIP, VPN
- Integrity - WPA, TKIP
- Network Segmentation - VLAN's
- Firewalls and Wireless DMZ
- Default Configuration Settings and Passwords
- Firmware Upgrades and Patching
- Remote Configuration and Management
- Role-Based Access Control
- Client Security
- Switches and Hubs
- Rogue Equipment (AP's and Clients)
- Controlling Signal Leakage
- Physical Security and Social Engineering
- Accessing Public Networks
- Safe SOHO Wireless Networking

## **Day 4 - Sundry WLAN Security Issues, Hacking Wireless Networks**

### **Sundry WLAN Security Issues**

- WiFi Protected Setup (WPS)
- 802.11w
- 802.11k and 802.11r for fast BSS transition
- 802.16 and WiMAX
- Proprietary Solutions
- RFID and VoWLAN
- Cellular Network Security
  - WWAN Generations
  - WAP and WML
  - PDA's and SmartPhones

### **Hacking Wireless Networks**

- Hacking and Information Security Backgrounder
- Wireless Security Assessments and Surveys
- Wireless Penetration Testing Methodology

- Information Gathering (Recon and Eavesdropping)
- Evading Detection and Bypassing Controls
- Gaining Access to the Network
- Port Scanning – Nmap (Demo)
- Vulnerability Scanning – Nessus (Demo)
- Exploiting Vulnerabilities
- Attack Types and Tools
  - Live Linux CD's – BackTrack (Demo)
  - Automated WEP Cracking – WEPBuster (Demo)
- Rogue Devices - AP's, Clients
  - Wired and Wireless Detection
- Man-in-the-Middle (MITM) Attacks
  - Setting up a Fake AP
  - "Evil Twin" with AirSnarf (Demo)
- Denial of Service Attacks (Void11)
  
- Lab #12 – Capture the Wireless Flag Contest

Contact Rui Pereira at [ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) or 1 (604) 961-0701 to book a place on the next presentation, or for further information. This document is also available online at [http://www.wavefrontcg.com/WirelessSec\\_2011.pdf](http://www.wavefrontcg.com/WirelessSec_2011.pdf).

Other security courses we offer include ["Secure Web Application Development and Testing"](#) and ["Ethical Hacking, Penetration Testing and Vulnerability Assessments"](#).