

Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA/CWSP, CPTS/CPTC
Principal Consultant, WaveFront Consulting Group
ruiper@wavefrontcg.com | 1 (604) 961-0701 | 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 (the hack was first disclosed by TJMaxx in January 2007). 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 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 \$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 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 and Bluetooth) 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 their own wireless networks;
- Identify (and fix) vulnerabilities and mis-configurations in major 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) will also be 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, ISP, 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

Course Outline

Day 1 - Introduction, Wireless Networks, Lab Environment, Cryptography for Wireless

Introduction

- The Threat Landscape
- Wireless vs. Wired Networks
- Wireless Network Attacks
 - Passive vs. Active Attacks
 - Man-in-the-Middle Attacks
 - Rogue Access Points
 - 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

Wireless Networks

- Wireless LAN Applications
- Wireless LAN Organizations
 - IEEE, Wi-Fi Alliance
- 802.11 Wireless Network Standards
- Bluetooth and Other Wireless Technologies

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

The Lab Environment

- Your Workstation
- Wireless Equipment
- Virtual Machines
- Lab #1 - Wireless Setup
- Windows Toolset
- Lab #2 – Using and Breaking MAC Address Filters

Cryptography for Wireless Networks

- Introduction to Cryptography
- Building Blocks
 - Symmetric and Asymmetric Cryptography
 - Block and Stream Ciphers
 - Message Digests and Message Authentication Codes (MAC's)
 - Public Key Infrastructure (PKI)
 - Hybrid Crypto-Systems
- Cryptography for Network Traffic
 - SSL and IPsec
- Key Management
- Attacking Crypto
 - Cryptographic and non-Cryptographic Attacks
 - Key Lengths

Security Concepts for Wireless Networks

- Security Requirements
 - Confidentiality, Integrity, Availability (CIA)
 - Authentication, Authorization, Accounting (AAA)
 - Protect, Detect, React, Recover
- Hacking and Information Security Background
 - Vulnerabilities, Exploits and Controls
- Wireless Security Assessments and Surveys

Day 2 - **Wireless LAN Discovery, WEP, WPA**

Wireless LAN Discovery

Passive and Active Scanning
 Authentication and Association
Discovery Tools
 NetStumbler and Inssider (Demos)
 Kismet (Demo)
Wireless Network Sniffing
 WireShark (Demo)
Lab #3 - WLAN Discovery (Netstumbler, Kismet)
Lab #4 - Wireless Sniffing (Wireshark)

WEP

WEP for Authentication and Confidentiality
How WEP Works
WEP Weaknesses
 Shared Keys and Key Management
 Cryptographic Implementation Issues
Hacking WEP
 Aircrack-ng (Demo)
Lab #5 - WEP Setup
Lab #6 - Hacking WEP (aircrack-ng)
Fixing WEP – TKIP and MIC

WPA

WPA1, WPA2, WPA-PSK and 802.11i
Authentication - 802.1X and EAP
 Supplicants and Authenticators
 EAP Authentication Types
 LEAP and PEAP
Lab #7 - WPA-PSK Setup
Hacking WPA-PSK
 Aircrack-ng (Demo)
 asLEAP and coWPATy (Demo)
Lab #8 - Hacking WPA-PSK (aircrack-ng)
Lab #9 - WPA Enterprise Setup (PEAP)

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

More Wireless Network Security

Virtual LAN's (VLAN's) and Network Segmentation
 AP Isolation and Guest Networks
SSID, Protocol and MAC Address Filtering
Lab #10 - Other Wireless Security Setup

- Securing the Upper Layers
 - Virtual Private Networks (VPN's)
 - Other Network Protocols (SSL, SSH, SNMP)
 - Management Interfaces
 - Captive Portals
 - Firewalls and DMZ's
- Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS)
 - Kismet, AirDefense
 - Rogue AP Detection
 - Intrusion Forensics
- Lab #11 – Configuring WIDS (Kismet)
- Protocol and Spectrum Analyzers
 - AirMagnet (Demo)
 - Wi-Spy (Demo)

Bluetooth Security

- BlueTooth Background
- BlueTooth Security Weaknesses
- Hacking BlueTooth
 - BTScanner (Demo)
 - BlueSnarfer
- A Bit about RFID

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
- Default Configuration Settings and Passwords
- Firmware Upgrades
- Remote Configuration and Management
- Role-Based Access Control
- Client Security
- Switches and Hubs
- Rogue Equipment (AP's and Clients)
- Controlling Signal Leakage
- Physical Security
- Social Engineering
- Accessing Public Networks

Day 4 - **Hacking Wireless Networks**

- Attack Types and Tools
- Information Gathering (Recon)
 - War Driving
- Rogue Devices - AP's, Clients
 - Wired and Wireless Detection
- Man-in-the-Middle (MITM) Attacks
 - "Evil Twin"
 - Airsnarf (Demo)
- Port Scanning – Nmap (Demo)
- Vulnerability Scanning – Nessus (Demo)
- Vulnerabilities and Exploits
- Live Linux CD's – BackTrack (Demo)
- Denial of Service Attacks
- Lab #12 – Capture the Wireless Flag Contest

Contact Rui Pereira at 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_2009.pdf.

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