

Control & Security of Wireless Networks

COURSE DURATION: 2-days

CPE HOURS: 16

LEVEL: Beginner / Group-Live

PREREQUISITES: None

ADVANCED PREPARATION: None

Wireless network implementations are growing at a tremendous rate. Our National Wireless Study demonstrated that only 33% of wireless networks are encrypted. This creates a serious security exposure for many organizations. Hackers can literally drive by a company's office building, detect the wireless network, park their car, connect to the network, and start penetrating systems – all automatically. This seminar explains the various technologies used in networks today and the inherent risks in each technology. The participants will learn how to identify specific wireless risks and install the proper countermeasures to mitigate the risk. The instructor will cover all of the major wireless technologies including 802.11, Bluetooth, cellular wireless (2 G, 2.5 G and 3 G). In addition, wireless application protocol will be explained to enable the participants to ensure that controls are built into wireless applications as they are developed. Each participant will also receive a copy of the Canaudit Wireless Network Audit and Security guide.

WHO SHOULD ATTEND

This seminar is intended for IT auditors, security officers, and network analysts. A basic understanding of telecommunications is a prerequisite.

SEMINAR OUTLINE

- | | | |
|--|--|--|
| <p>I Introduction</p> <ul style="list-style-type: none">• Initial security concerns• Review results of Canaudit's national "war driving" study• Wireless an inevitable• Security starts early | <p>IV Defeating 802.11 Controls</p> <ul style="list-style-type: none">• Hacking made easy• War driving• Cracking WEP encryption• Navigating the internal network• Compromising network devices and servers• Risk/Control tables & Checklists | <ul style="list-style-type: none">• Evolution generation (2.5 G)• Third Generation (3 G)• Universal Mobile Telecommunications Service (UMTS)• Risk/Control tables & Checklists |
| <p>II Wireless Applications – The Tip of the Iceberg</p> <ul style="list-style-type: none">• LAN access and mobility ports• Email and Internet access• Banking & financial services• Retail applications• Medical applications• Hotel and travel uses• Outbound logistics applications | <p>V Bluetooth Wireless Communications</p> <ul style="list-style-type: none">• System Architecture• Spread spectrum technology• The Bluetooth Protocol Stack• Middleware protocols• Bluetooth Profiles<ul style="list-style-type: none">➢ Generic access profile➢ Telephony profiles➢ Serial & object profiles➢ File transfer profile➢ Dial up networking➢ LAN access profile• Risk/Control tables & Checklists | <p>VII Wireless Application Protocol (WAP)</p> <ul style="list-style-type: none">• Business case for WAP• When to use WAP• WAP user interfaces• Push and pull technologies• Securing WAP applications• Controlling WAP applications• Risk/Control tables & Checklists |
| <p>III Wireless LANS – 802.11 Technology</p> <ul style="list-style-type: none">• Overview of the 802.11 standards• Architecture• Protocol• MAC service data units• Message distribution• Authenticating and deauthenticating devices• Encryption (WEP)• Basic configuration• Access points• Frequency hopping• Protecting wired network assess• Risk/Control tables & Checklists | <p>VI M-Commerce Technology</p> <ul style="list-style-type: none">• Fundamentals of mobile communications• Basic network architecture• Air interface techniques• Roaming issues• Handoff/handover issues• Second generation wireless (2 G) | <p>VIII Building the Wireless Risk Assessment</p> <ul style="list-style-type: none">• Test is really production• Identifying wireless networks• Cataloging wireless applications• Performing a risk assessment• Preparing the management briefing |
| | | <p>IX The Canaudit Wireless Network Audit & Security Guide</p> |