

## Wireless LAN Security: Attacks and Countermeasures

ISACA Hong Kong  
May 6 2003

John Lauderdale  
Global Risk Management Solutions  
Tel: +852 22892926  
John.Lauderdale@hk.pwc.com



## Outline

1. Introduction
2. Problems with 802.11 security
3. Attacks on and risks to Wireless Networks
4. Defending wireless networks

### Demos:

- WLAN Discovery
- Eavesdropping
- WEP cracking
- Fake Access Point

## The case for wireless networking

### Wireless benefits

- Increased productivity, lower installation cost, greater flexibility
- Used by hospitals, universities, airports, hotels and retail shops.
- Ad-hoc networks enable network connectivity and data synchronization

**Risks of wireless networks = risks of wired networks + new risks introduced by weaknesses in wireless protocols.**

**Wireless LANs can be the logical equivalent to having an Ethernet port in a parking lot or on the street**

3

## Access points and network cards

### • Access Point (AP)

### • Network Cards



4

## Introduction: OSI layers and 802 structure

	802 LLC			
OSI data-link layer	802.11 MAC			
OSI physical layer	802.11	802.11b	802.11g	802.11a
<b>Max Data Rate</b>	2 Mb/s	11 Mb/s	22 Mb/s	54 Mb/s
<b>Frequency</b>	2.4 GHz and IR	2.4 GHz	2.4 GHz	5 GHz
<b>Modulation</b>	FHSS and DSSS	DSSS	OFDM	OFDM

5

## Introduction: WLAN technologies

### Infrastructure mode vs.

- One cell provides Basic Service Set (BSS) service
- Many cells working together provides Extended Service Set (ESS)

### • Range

- 50 Meters indoors to 1500 Meters outdoors
- Directional antennas can enable access from tens of kilometers

### • 11 Channels

- Channels 1, 6, and 11 are non-overlapping

### • Signal strength determines the speed and transmission distance

6

## Introduction: Antennas

- Antennas
  - Omni-directional
  - Sector
  - Uni-directional



Antenna images courtesy of www.hyperlinktech.com

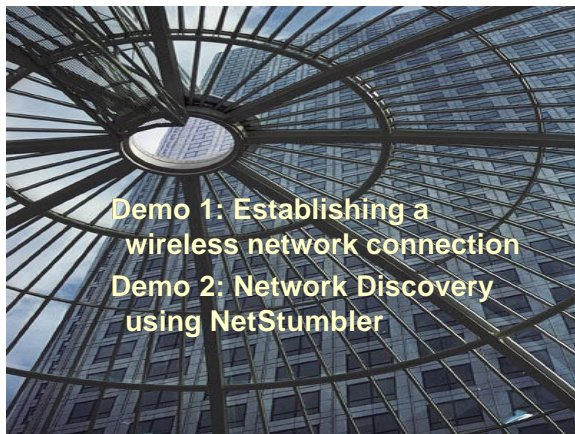
## Establishing a WLAN connection

- 802.11 network Basic Service Set (BSS)
  - Central access point (AP) and client stations.
- BSS is identified with as service-set identifier (SSID).
- WLAN infrastructure mode connection:
  - AP sends out beacon packets every few seconds with SSID/BSID.
  - Network card detects AP, displays the SSID, and gives the user the option to associate with it.
  - The station and AP go through a handshake and authentication process and make the connection



8

PRICEWATERHOUSECOOPERS



## WLAN discovery using NetStumbler

- NetStumbler runs on Windows
- Puts network card into monitoring mode
- Scans all eleven channels to identify active network traffic / SSIDs
- Monitors but does not record transmitted data

Used for:

- "War Driving"
- "War Chalking"
- "War Flying"

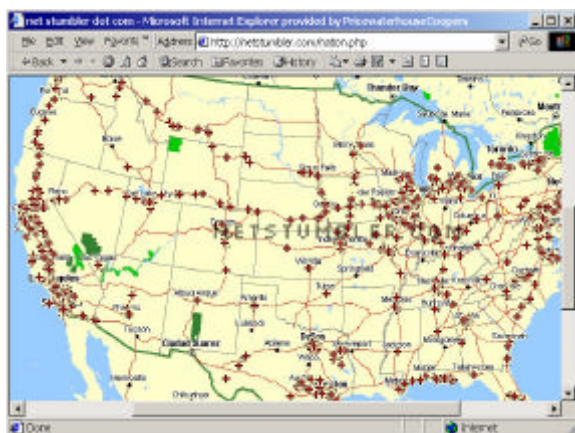
Data can be uploaded to a centralised database

Records

- MAC address
- SSID
- Network name
- Network channel
- Equipment vendor
- Connection type
- Whether WEP encryption is used
- SNR
- GPS latitude, longitude
- Time first seen, time last seen
- Charts signal strength histogram

10

PRICEWATERHOUSECOOPERS



## Wired Equivalent Privacy (WEP)

- WEP designed to secure wireless link only, not end-to-end security
- Provides
  - Authentication
  - Confidentiality
  - Integrity
- Does not provide
  - Audit, authorisation, or non-repudiation

WEP Encryption keys

- 40 bit (5 ASCII characters),
- 104 bits (13 ASCII characters), or
- 140 bits (only with some implementations)

40 or 104 bits → 24 bits



Encryption Key



Message

12

PRICEWATERHOUSECOOPERS

## Typical security problems with 802.11 security

Security features not enabled by default.

Use of short IVs.

Use of short 40 bit keys.  
Shared crypto keys.

*Crypto keys cannot be updated automatically and frequently.*

Poor packet integrity.

*Device authentication is simple shared key challenge-response.*

Authentication is not enabled; simple SSID identification occurs.

*The client does not authenticate the AP.*

13

PRICEWATERHOUSECOOPERS

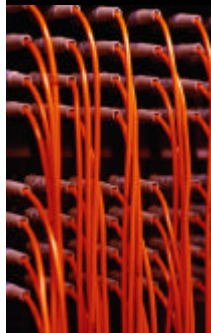
## Risk: Loss of Confidentiality

- Interception of wireless signals
  - Ease of signal access
  - Physical controls less effective
  - Difficult to control signal transmission distance: transmission may be outside the building
- Passive eavesdropping
  - Disclosure of sensitive network information, User Ids, Passwords, configuration data
- Rogue access points may be placed by an insider.
- Signals can be detected from the street
- Network sniffer / analyser
  - Captures network traffic
  - Effective because WEP is often not used and can be broken.
- Wireless packet analysers can automate the process of capturing and analysing network traffic.

14

PRICEWATERHOUSECOOPERS

## Risk: Loss of Confidentiality (cont)



- Monitoring
  - Sniffing traffic sent between the access point and the main part of the network if it is connected using a hub.
- Rogue access points
  - A malicious or irresponsible user can put a rogue access point in a closet, under a conference room table, or any other hidden area of a building.
  - Rogue APs are usually a surprise to the IT Dept.
  - May enable unauthorised network access.
  - May enable authorised users to get access through an unauthorised channel.
  - It may be difficult for most users to tell the difference between real and rogue access points.

PRICEWATERHOUSECOOPERS

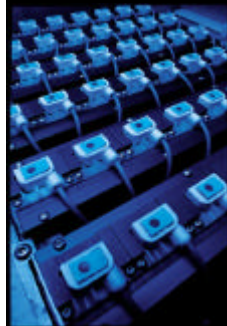
## Risk: Loss of Integrity



- Loss of integrity
  - Possible when encryption is not used.
  - WEP integrity is checked using CRC which can be easily modified

PRICEWATERHOUSECOOPERS

## Risk: Loss of Integrity (cont)



- Denial of Service
  - Radio jamming results in communication breakdown
  - Microwave or cordless phone interference
  - Unintentional DoS may result from monopolising a wireless signal by downloading a large file (consider restricting the amount and type of data allowed over wireless networks)

PRICEWATERHOUSECOOPERS

## Risks of wireless connections via third party networks

- Connectivity using third-party wireless networks (airports, hotels, coffee shops)
  - Malicious users access public networks
  - Untrusted public networks bridge users own network, possibly allowing anyone on the public network access to the bridged network.
  - High gain antennas increase the chance of eavesdropping by increasing coverage area.
- When connecting via third-party networks, additional encryption should be used.

16

PRICEWATERHOUSECOOPERS

## “Hacker mischief “ / Wireless network risks

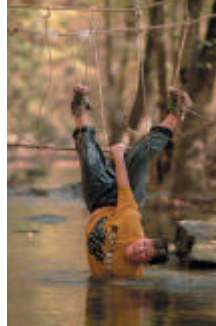


Wireless networks may be put at risk by someone trying to...

- Get unauthorised access to the internal network.
- Steal and disclose sensitive information transmitted unencrypted over the air.
- Launch a DoS attack against wireless connections or devices.
- Steal the identity of network users.
- Corrupt sensitive data sent over WLAN or on the network.
- Use rogue access points to gain sensitive information.

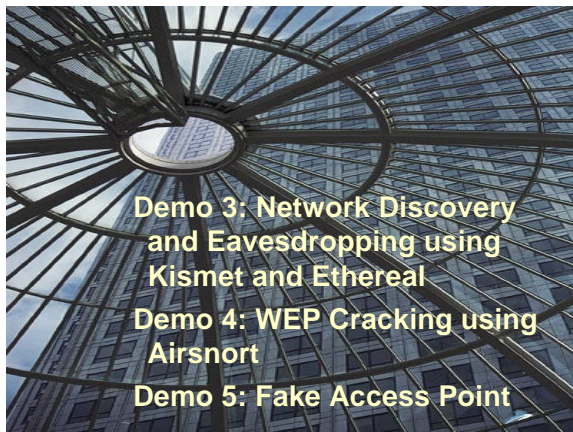
PRICEWATERHOUSECOOPERS

## Hacker “mischief” / wireless network risks.



7. Violate the privacy of WLAN users and track their actions.
8. Load a virus on a wireless device which will later get onto the network.
9. Use wireless connections to access a company's network, then launch attacks on other networks.
10. Access and compromise network management controls.
11. Use a third-party un-trusted WLAN to access a company network.
12. Attack ad-hoc transmissions.

PRICEWATERHOUSECOOPERS



**Demo 3: Network Discovery  
and Eavesdropping using  
Kismet and Ethereal**  
**Demo 4: WEP Cracking using  
Airsnort**  
**Demo 5: Fake Access Point**

## Network eavesdropping using Kismet

### Kismet

- Linux based
- Multi-tier architecture with separate Kismet Server and User interface
- Monitors traffic on 11 channels
- Captures traffic (including weak WEP IVs) for later analysis
- Detects all types of wlan connectivity.
  - Probe, Access points, Ad-hoc connections
  - Detects vulnerable factory configurations

### Kismet Features

- Multiple packet sources
- Channel hopping
- IP block detection
- Cisco product detection via CDP
- Ethereal/tcpdump compatible file logging
- Airsnort-compatible “interesting” (cryptographically weak) logging
- Hidden SSID de cloaking
- Grouping and custom naming of SSIDs
- Multiple clients viewing a single capture stream
- Graphical mapping of data (gsmmap)
- Cross-platform support (handheld/linux and BSD)
- Manufacturer identification
- Detection of default access point configurations
- Detection of Netstumbler clients
- Runtime decoding of WEP packets
- Multiplexing of multiple capture sources

22

PRICEWATERHOUSECOOPERS

## WEP Cracking using Airsnort



- Takes advantage of Key scheduling algorithms implemented with RC4
- Monitors network traffic and computes encryption keys after at least 100 Mb of network packets have been sniffed.
  - May take 3-4 hours on a saturated network
  - May take a few days on a low usage network
  - WEP keys can be generated in less than one second after enough traffic is captured.
  - Used for WEP key discovery which enables confidentiality and integrity to be compromised.

23

PRICEWATERHOUSECOOPERS

## Management Countermeasures



### 1. Develop WLAN Usage policies

- What information can be sent over WLAN links?
- Who can use it?
- For what purpose?
- What standard security settings should be applied to PCs connecting to Wireless networks?
- Where can it be used?
- Encryption requirements? Hardware requirements? Software requirements?
- Frequency and scope of security assessments?
- Encryption and key management?

PRICEWATERHOUSECOOPERS

## Operational Countermeasures



2. Conduct wireless security audits
  - Use wireless site survey tools to measure signal range
3. Implementing physical security
  - access controls
  - boundary protection

PRICEWATERHOUSECOOPERS

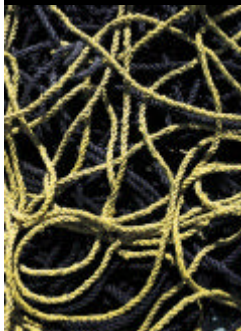
## Technical Countermeasures

5. Secure Access points
  - Configure administrative passwords
    - No default passwords
    - Consider 2factor authentication
    - Ensure cryptography (SSL) is used when configuring devices
  - Use strong Encryption
    - Use strongest available (104 bit or more)
  - Control the reset function
  - Use static IP addresses (not DHCP) for small networks
  - Assign Ethernet MAC Access Control Lists (ACLs) for small networks
    - Restricts the network cards that can connect
  - Change SSID from the factory default
  - Disable SSID broadcast or reduce its interval

26

PRICEWATERHOUSECOOPERS

## Technical Countermeasures



- Access point Configuration
  - Disable SNMP or use SNMP v3 which has stronger authentication
  - Change SNMP community string from "public"
- Change the default channel (1,6,11)
- Implement strong authentication
  - Usernames/passwords, smartcards, biometrics, PKI

PRICEWATERHOUSECOOPERS

## Technical Countermeasures



6. Keep Access Points Secure
  - Software patches and upgrades
    - Periodically check for software updates
    - Keep an eye on new technology to overcome WLAN shortcomings
      - 802.11x
      - 802.11i-Robust Security Network

PRICEWATERHOUSECOOPERS

## Technical Countermeasures

7. Implement personal firewalls
8. Implement Intrusion Detection System (IDS)
  - Understand the limitations of Network and Host IDS
    - Attacks on wireless clients may go undetected
    - Network IDS may not detect Datalink level DoS attacks
  - Consider using wireless IDS which can:
    - Detect unauthorised peer-to-peer communications
    - Detect rogue access points
    - Identify physical location of wireless devices within buildings
    - Allow analysis and monitoring of wireless communications

29

PRICEWATERHOUSECOOPERS

## Wireless Assessments



- Wireless Assessments
- Checks wireless security posture
  - Uses wireless network analysers and other tools.
  - Checks for rogue access points and other unauthorised access
  - Can be combined with penetration testing
  - Consider using independent third parties for wireless assessments, who may
    - Be more up to date on security vulnerabilities
    - Be better trained on wireless security
    - Use more up-to-date tools

PRICEWATERHOUSECOOPERS

## Summary: Key points

- Like any new technology, implementing Wireless networks brings benefits but also new and increased risk.
- Wireless technology drives the need for better internal security.
- Companies should prohibit the use of wireless networking technology unless they are prepared to implement the procedural, operational and technology needed to mitigate known risks.
- There are wireless risks even if you are not planning to implement wireless technology.
  - Rogue access points
  - New phones, PDAs, laptops come with built-in WLAN and bluetooth capabilities.
  - Users are buying WLAN cards for use at home and leaving them in their laptop when they take them to the office. This can provide a backdoor into the network.

31

PRICEWATERHOUSECOOPERS 

PRICEWATERHOUSECOOPERS 

## Questions?

John Lauderdale  
Global Risk Management Solutions  
Tel. +852 22892926  
John.Lauderdale@hk.pwc.com

## Wireless LAN security mini-checklist

1. Develop wireless LAN policies standards, procedures and guidelines.
2. Understand how the overall network architecture is affected by Wireless LAN technology; will use of wireless connectivity put your network at risk?
3. Label and keep an inventory of all wireless and handheld devices
4. Perform periodic wireless security assessments. This should include ongoing, randomly timed security audits to monitor and track wireless and handheld devices.
5. Enable wireless security features. Routinely test that the preventive and detective controls are working properly.
6. Design and implement a defence-in-depth strategy using built-in security features.
7. Apply patches and security enhancements. Be sure to change factory default security settings.
8. Implement a holistic security architecture that includes the use of firewalls, cryptography, and IDS.
9. Standardize security configurations, based on the policy.
10. Implement configuration / change control and management to ensure the latest software releases and security configuration enhancements have been applied to all equipment.
11. Provide security training to raise awareness about security issues surrounding wireless technologies.
12. Vigilantly monitor new threats and vulnerabilities associated with wireless technologies.

33

PRICEWATERHOUSECOOPERS 