pentest
security assurance

Wireless Threats To Corporate Security

A Presentation for ISACA UK Northern Chapter

Introduction

- Who are we?
  - Matt Moore, Senior Consultant @ PenTest Ltd.
  - Mark Rowe, Technical Director @ PenTest Ltd.
- What do we do?
  - Security Consultants specialising in vulnerability assessment and Penetration Testing.
  - Active Security Researchers.
  - Contributors to various open source security projects.

Outline

- Overview of Wireless Technologies.
- Risks inherent to Wireless connectivity.
- Demonstration of wireless security flaws using freely available tools.
- Implementing Wireless Security.
- Summary.
- Questions.

pentest
security assurance

What do you mean 'Wireless'?

- Wireless devices use Radio Frequency (RF) technology to facilitate communication.
- Various types of wireless communication solutions use different frequencies, most regulated by governments.
- 802.11 and Bluetooth operate in the 2.4Ghz unregulated band.

Common wireless usage scenarios.

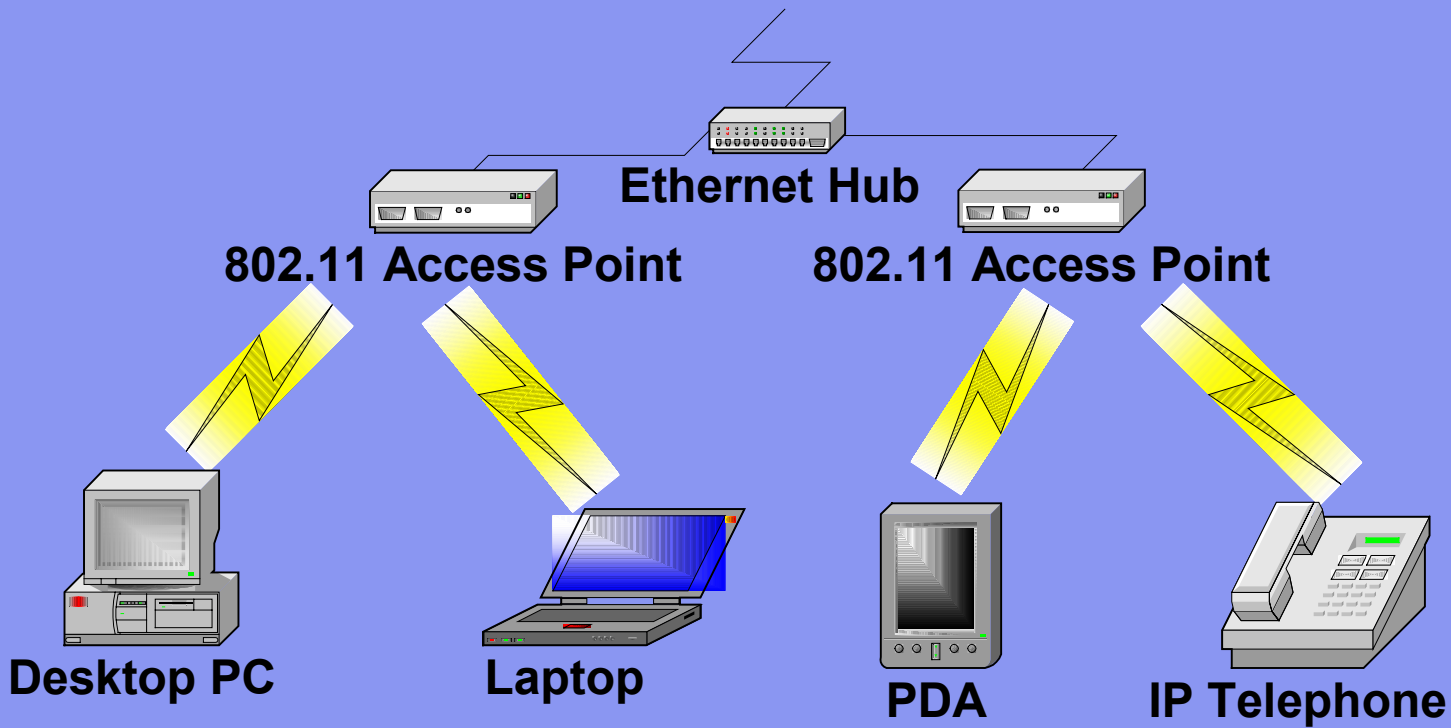
- Wide Area Networks (WANs) using GPRS, GSM etc.
- Local Area Networking (LANs) using 802.11b (aka Wi-Fi).
- Personal Area Networking (PANs) using Bluetooth.

802.11 (aka Wi-Fi) Wireless LAN

- What is it?
  - Medium range. Around 150-200ft, in most cases.
  - Can be extended using directional antenna, repeaters etc.
  - 802.11b is most widely used standard today.
- Benefits
  - Removes need for cabling infrastructure.
  - Rapid deployment.
- How does it work?
  - Clients 'associate' to 'Access Points' (AP's) – Infrastructure Mode.
  - Clients form peer-to-peer network - 'Ad-Hoc' Mode.

pentest
security assurance

802.11 Wireless Local Area Network (LAN)

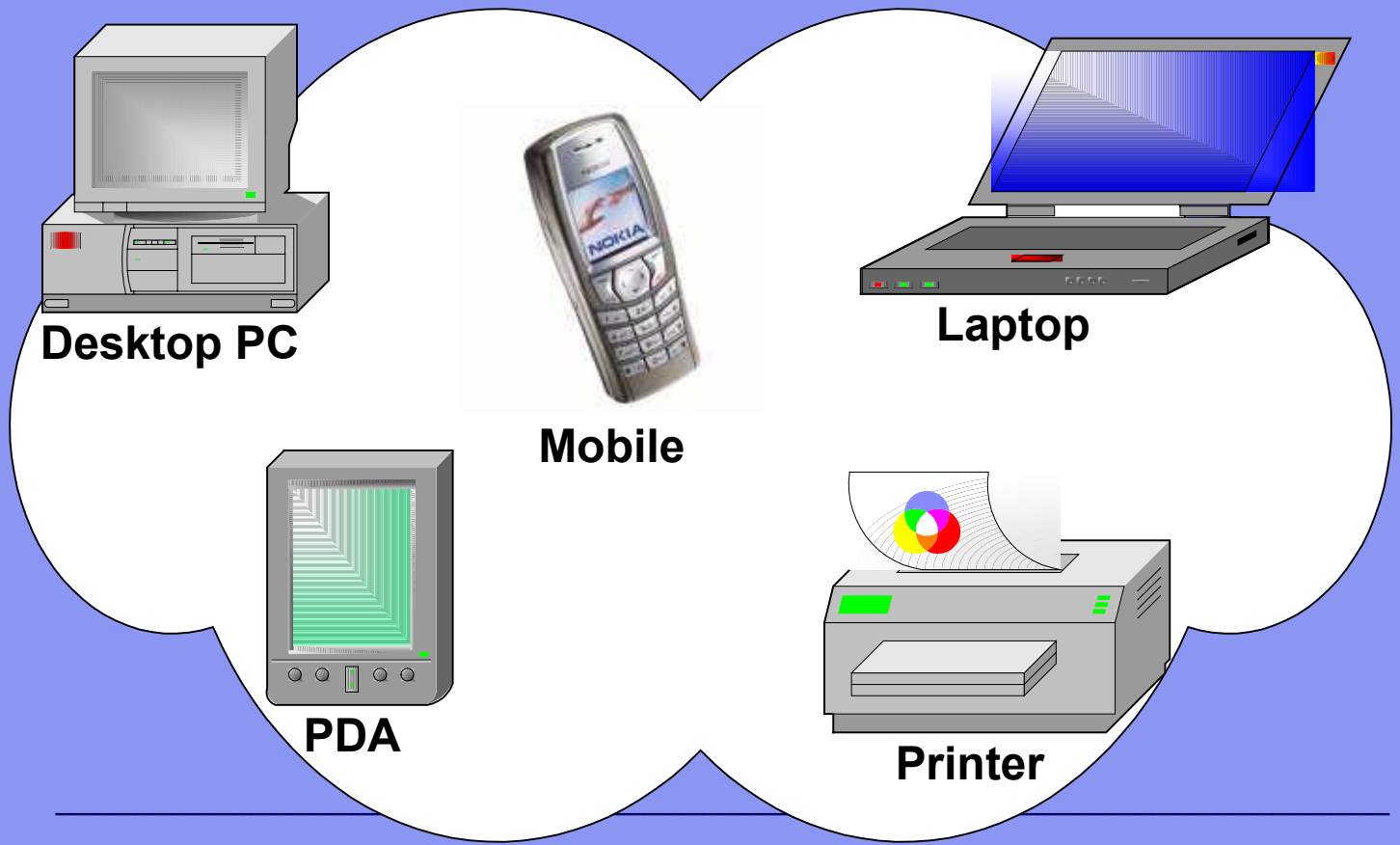


Bluetooth Personal Area Network (PAN)

- Short range (around 10m or 30 feet).
- Short range cable replacement technology, used to transmit both voice and data:
  - Syncing PDA's.
  - Wireless Mobile Phone Headsets.
  - Audi Car Phone.
  - Phillips Fridge(!)
- Gadget-oriented.

pentest
security assurance

Bluetooth Personal Area Network (PAN)



Where is wireless used today?

- Retail - Handheld stocktaking devices in supermarkets and warehouses.
- Medical – Doctors use PDA's to access patient records whilst on ward.
- Hospitality – Hotels / Coffee Shops / Airports increasingly providing 802.11b broadband internet access.
- Corporate IT Infrastructure.
  - Allows employees to access network resources from anywhere in the building (e.g. meeting rooms).
  - Allows employees to synchronise PDA's.

Wireless usage is increasing…

- Cost of hardware dropping quickly.
- Connectivity available in airports, coffee shops etc.
- Frequency of wireless security assessments for clients has increased.
- Bluetooth / 802.11b networking included as standard with many new products
  - Phones
  - Laptops

Generic Wireless Security Problems

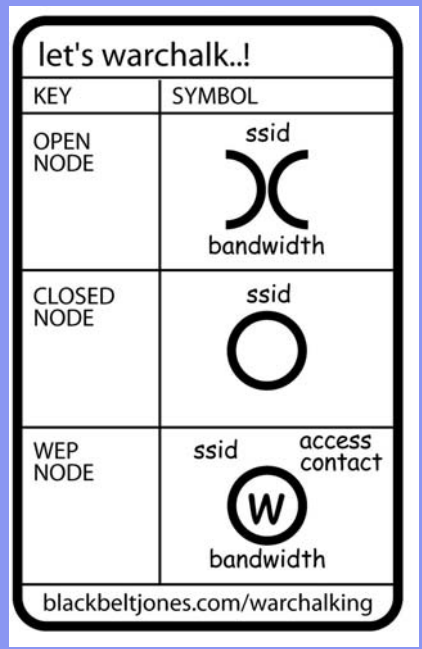
- Over-the-air communications inherently insecure.
- Physical access to networks / devices not required.
- Facilitates anonymous attacks.
- Devices authenticated rather than users.
  - Risk of stolen devices.
- All of the usual threats / risks apply:
  - Confidentiality.
  - Integrity.
  - Availability.

802.11b Security Problems

- 'WarDriving'.
  - Extensively reported in media.
  - Easy to discover 802.11 access points.
  - Default configuration of AP's.
  - 'Rogue' Access Points.
- New technology.
  - Common misconceptions about security.
  - Cheap hardware, free software.
  - Anonymous.

802.11b Security Problems

- 'Warchalking' (www.warchalking.org)



802.11b Security Problems

"Leeds, UK. Managed to find several open nodes in Leeds, and I've only really driven within 2 miles of my house...The Innovation Centre has a nice phat pipe, open to the world, and a lovely garden in which to sit whilst using it :) … There are 2 networks near "Joseph's Well" but the signal is very weak from the road (I suspect at least one of these is an NHS node) .... I'll be chalking them all tonight!"

Does 802.11b have no security?

- WEP ('Wired Equivalent Privacy')
  - Allows encryption of data portion of packets.
  - Vulnerable to attack
    - Passive attacks, based on statistical analysis.
    - Depending on size of network, can 'break' rather quickly.
    - Tools exist to perform the attack. (airsnort, wepcrack)
  - No key management / distribution facilities.
  - Authentication via shared key.
  - Shared keys quickly compromised.

Does 802.11b have no security?

- Other security solutions are often proprietary and specific to particular vendors. (e.g. Cisco LEAP)
- Not compliant with Wi-Fi standard.
- Other solutions:
  - Use VPN / SLAN technology as well.
  - IPSec
  - 802.1x / RADIUS
    - Supported in WinXP / Internet Authentication Server (IAS)

Demonstration – Netstumbler

- Netstumbler
  - Supports most Wi-Fi cards.
  - Identifies presence of Wi-Fi networks and can identify client probes.
  - GPS enabled.
  - Shows signal strength.

Sniffing Wireless Networks

- Snooping on network traffic
  - Topology.
  - Technologies in use.
  - Confidential information.
  - Various Commercial and free tools.
    - AiroPeek
    - Kismet

Kismet Demonstration

- Kismet
  - Free tool, available for Linux.
  - Allows sniffing of 802.11 network traffic.

More 802.11 weaknesses…

- MITM attacks possible (airjack)
  - IPSec
  - SSH
- Base Station Cloning
- Default WEP Keys
- Jamming (Denial of Service)
  - Unregulated band, interference can be unintentional (Microwaves, Bluetooth, Baby minders etc)
- 'Ad-Hoc' Mode 802.11b Networking
  - Exposes client devices.
  - Another potential route into the network.

Wireless Enabled PDA's and Security

- Insecure configuration of wireless-enabled PDA's.
  - Another potential risk to corporate security.
  - May contain sensitive business information
    - HP / Compaq IPAQ Bluetooth / Wi-Fi enabled PocketPC.
  - Possible threat from malicious code in future.
  - Post-XMAS increase in system support calls.

pentest
security assurance

Implementing Wireless Security

- Well designed architecture
  - Physical placement of AP's.
  - Outside firewall.
- Use additional layers of security (e.g. VPN).
- Define clear PSPG for wireless use within org.
- Educate staff.
- Regular security assessments.
- Consider wireless IDS systems (AirDefence).
- Upcoming improvements to wireless security.

Where to next?

- Future wireless standards are looking to address the security problems.
- WiFi Protected Access (WPA) interim solution.
  - Subset of upcoming 802.11i standard.
  - Improves authentication and integrity mechanisms.
  - A replacement for WEP.
  - Backward and forward compatible.
  - Two modes of operation (Enterprise or Home).
- Another botched bolt-on fix?
- 802.11i provides key management, stronger authentication and a variety of other improvements.

Summary

- Immature technologies.
- Incredibly useful, with many obvious benefits.
- Will become ubiquitous within a few years despite security concerns.
- Should not be considered suitable for carrying security sensitive information at the moment.
- Future standards attempt to address security – how well they do this remains to be seen.