Datacraft

Today's challenge on Wireless Networking

David Leung, CISM
Solution Consultant, Security
Datacraft China/Hong Kong Ltd.

Agenda

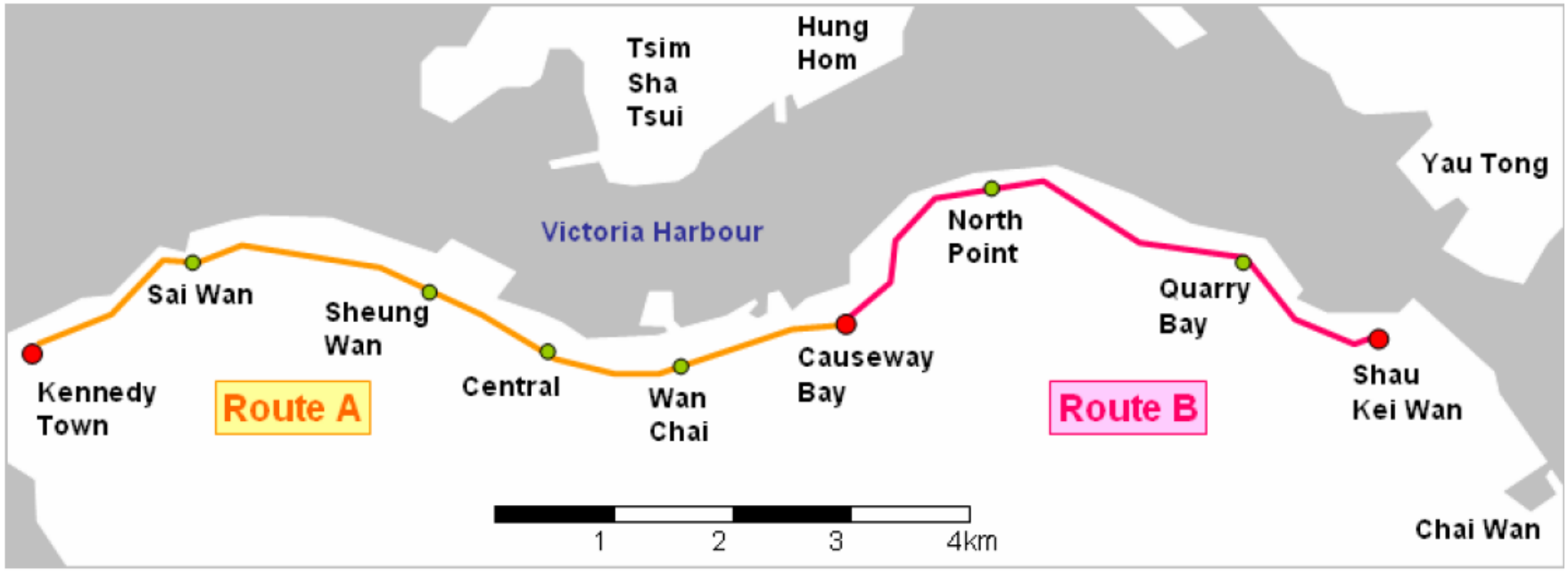
Datacraft

- How Popular is Wireless Network?
- Threats Associated with Wireless Networking
- Wireless Security – the Revolution
- Layered Wireless Security Approach
- Maintaining Good Health - Wireless Assessment

How Popular is Wireless Network?

Datacraft

War Driving 2007 – PISA

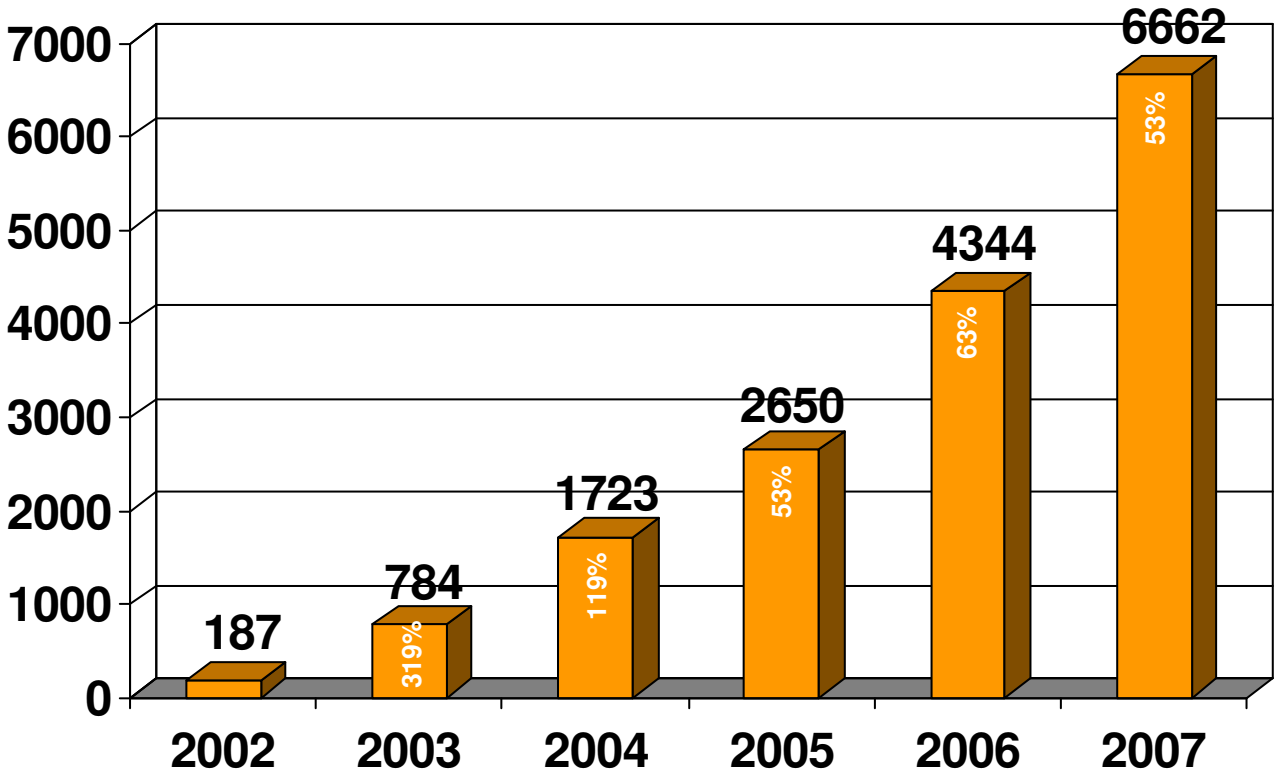


War Driving Route

How Popular is Wireless Network?

Datacraft

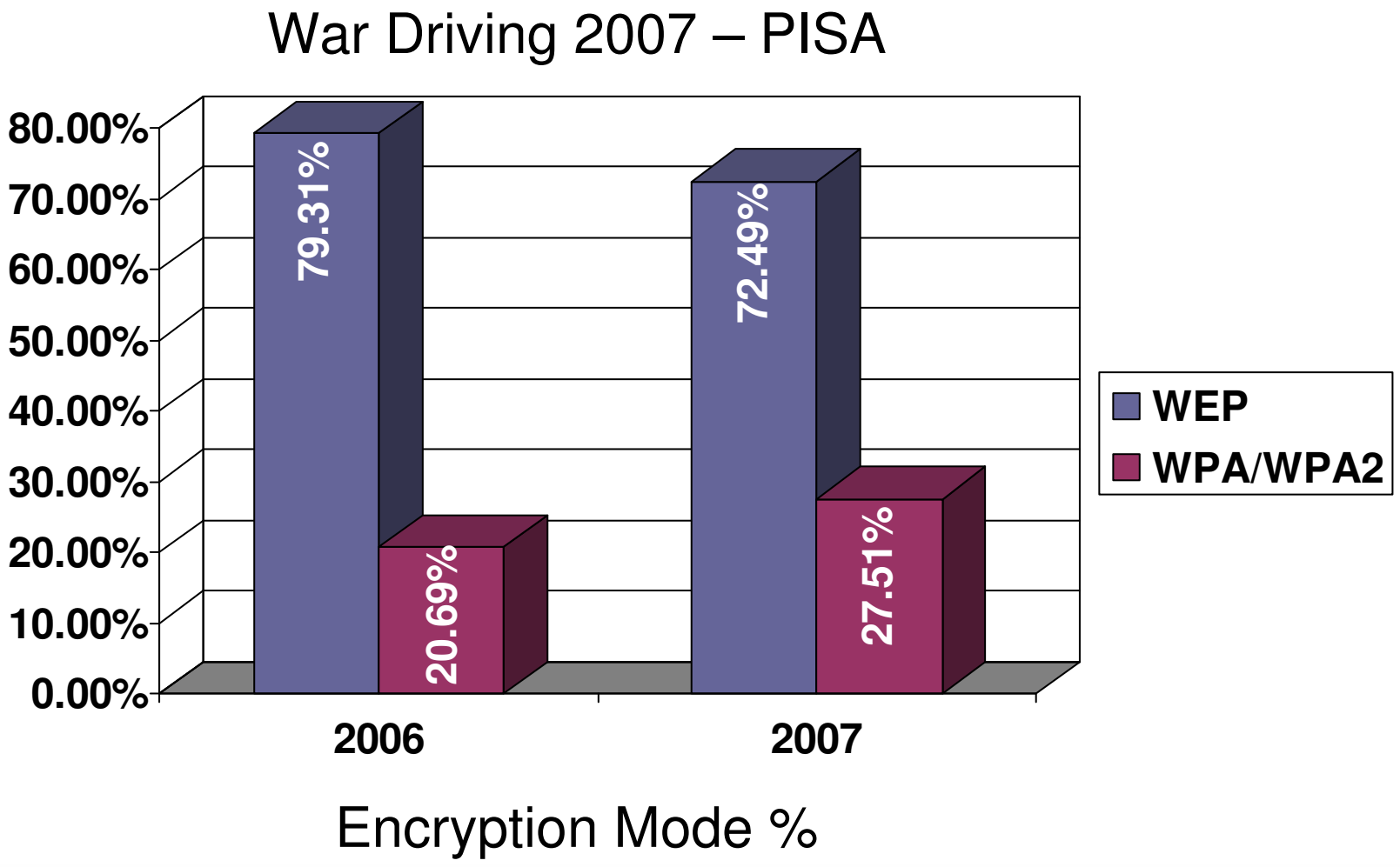
War Driving 2007 – PISA



No. of APs discovered

How Popular is Wireless Network?

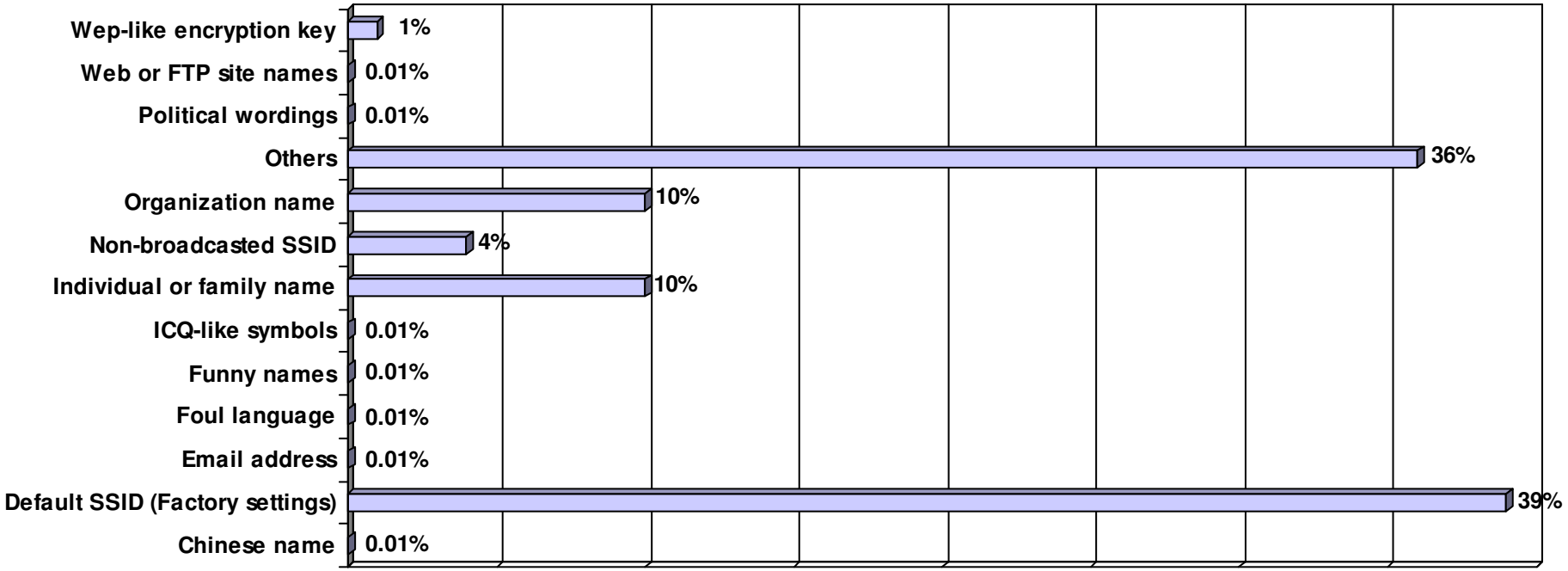
Datacraft



How Popular is Wireless Network?

Datacraft

War Driving 2007 – PISA



SSID Analysis

Wireless Security – the Revolution

Datacraft

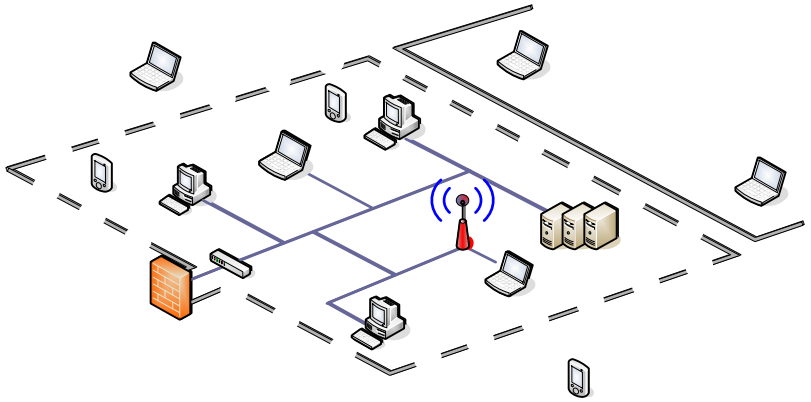
Traditional Network Environment

Protection focused on Network Entry Point (Outside-In)

- Firewall
- VPN
- 2-factor logon

Less worried on internal

- Bounded by Physical Protection
- Less likelihood on internal security incidents
- End point security for road runners
- Standardized H/W, O/S, applications



As Wireless Network Deployed
The Network Becomes Boundaryless

Physical boundary have been removed

- No more walls to protect your NETWORK
- Radio signal leakage
- Insufficient planning
- Mis-configurations

Wireless Networking is Invisible!

Wireless Security – the Revolution

Datacraft

WiFi Encryptions – How secure they are?

- WEP (Wired Equivalent Privacy)
  - Shared Key: 64 or 128-bit WEP Key (24-bit IV included)
  - Packet encrypted by RC4 streams
  - Security weakness
    - Short Key size (2^{20} RC4 keys)
    - IV collisions or altered packets
    - Can be cracked within hours

- WPA2 (WiFi Protected Access)
  - Created in response to serious weaknesses found in WEP
  - Personal
    - 8 to 63 character Pre-shared Key
  - Enterprise
    - 802.1X authentication / Radius (individual has their own password)
  - TKIP or AES encryption
    - Technically more secure

Threats Associated with Wireless Networking

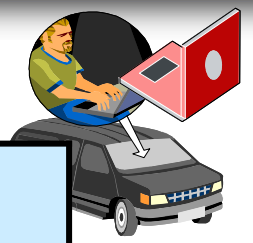
Datacraft

Identity Theft

- Spoofing – Mac Address, SSID etc.
- Breaking encryption
  - 50% successful rate with 40,000 packets
  - 95% successful rate with 85,000 packets
  - 104-bit WEP key can be break within 3 seconds with 40,000 packets
  - Hacking tools on wireless client WEP Cracking, not AP anymore
    - The Café Latte Attack
    - WepOff

Threats Associated with Wireless Networking

Datacraft



Network Configuration	Approximate Cracking time
Shared + DHCP	~ 6 minutes
Shared + Static IP	~ 6 minutes
Open + DHCP	~ 6 minutes
Open + Static IP	~ 6 minutes

Probing & Association with target victim

Send numerous ARP Requests to victim

Collect sufficient ARP Respnonses for WEP Cracking

Threats Associated with Wireless Networking

Datacraft

Denial-of-Service Attacks

- Aim to prevent legitimate users from accessing network resources – loss of production
- DoS on perimeter of Network (e.g. F/W, Mailserver etc.)
  - Single point of attack, single point of protection
  - Most F/W and Anti-Spam can block malicious connections
- How about multiple point of attacks = multiple point of protection
  - Jamming Wireless Signal in a matter of seconds
  - Your internet connections still works…….but you users can't access it.
  - Heavy workload to IT Support
  - Again, No trace at all

Datacraft

How easy to crack WEP?

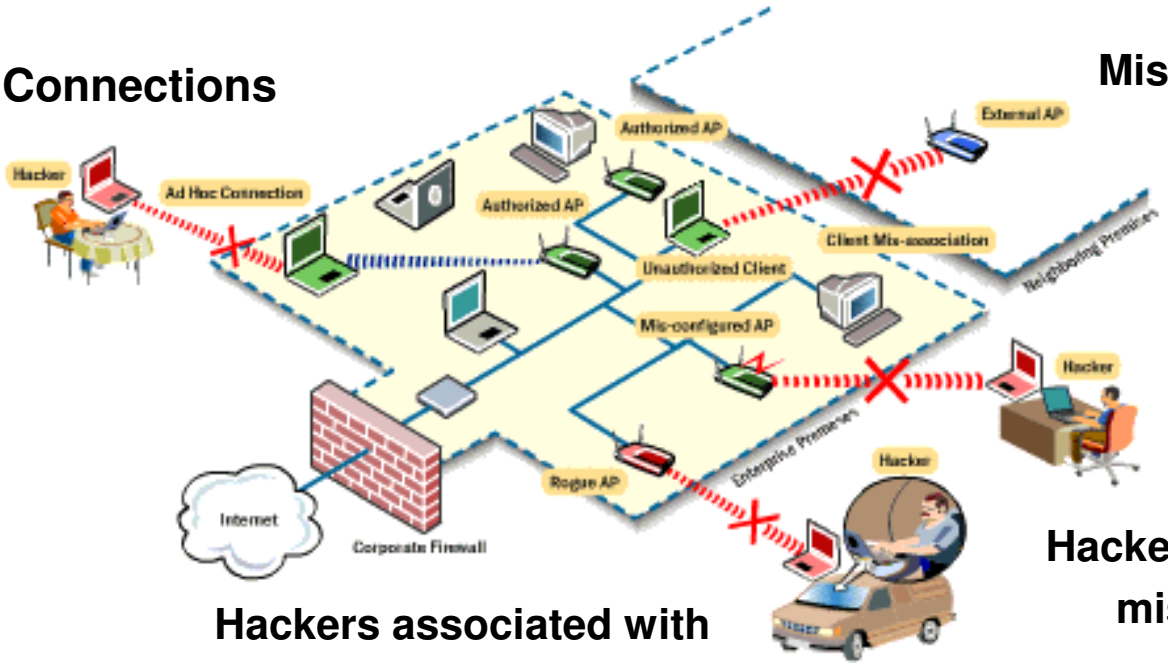
1. Setup equipment
   - a Computer
   - WiFi card that supports monitoring mode and packet injection
   - Market available tools e.g. Backtrack CD
2. Find the target (SSID)
   - Airdump-ng
   - Net Stumbler
3. Capture Data from Air
   - Airmon-ng
   - Airodump-ng
4. Wait……..or make the network busy
   - Aireplay-ng
   - Packetforge-ng
5. Crack WEP key with Captured Data
   - Aircrack-ng

Threats Associated with Wireless Networking

Datacraft

Scary enough!? What more is coming!

Ad Hoc Connections



Mis-association with external APs

Hackers associated with Rogue APs

Hackers associated with mis-configured APs

New Wireless Security Approach

Datacraft

New Wireless Security Approach

Datacraft

1) Securing Wireless Devices

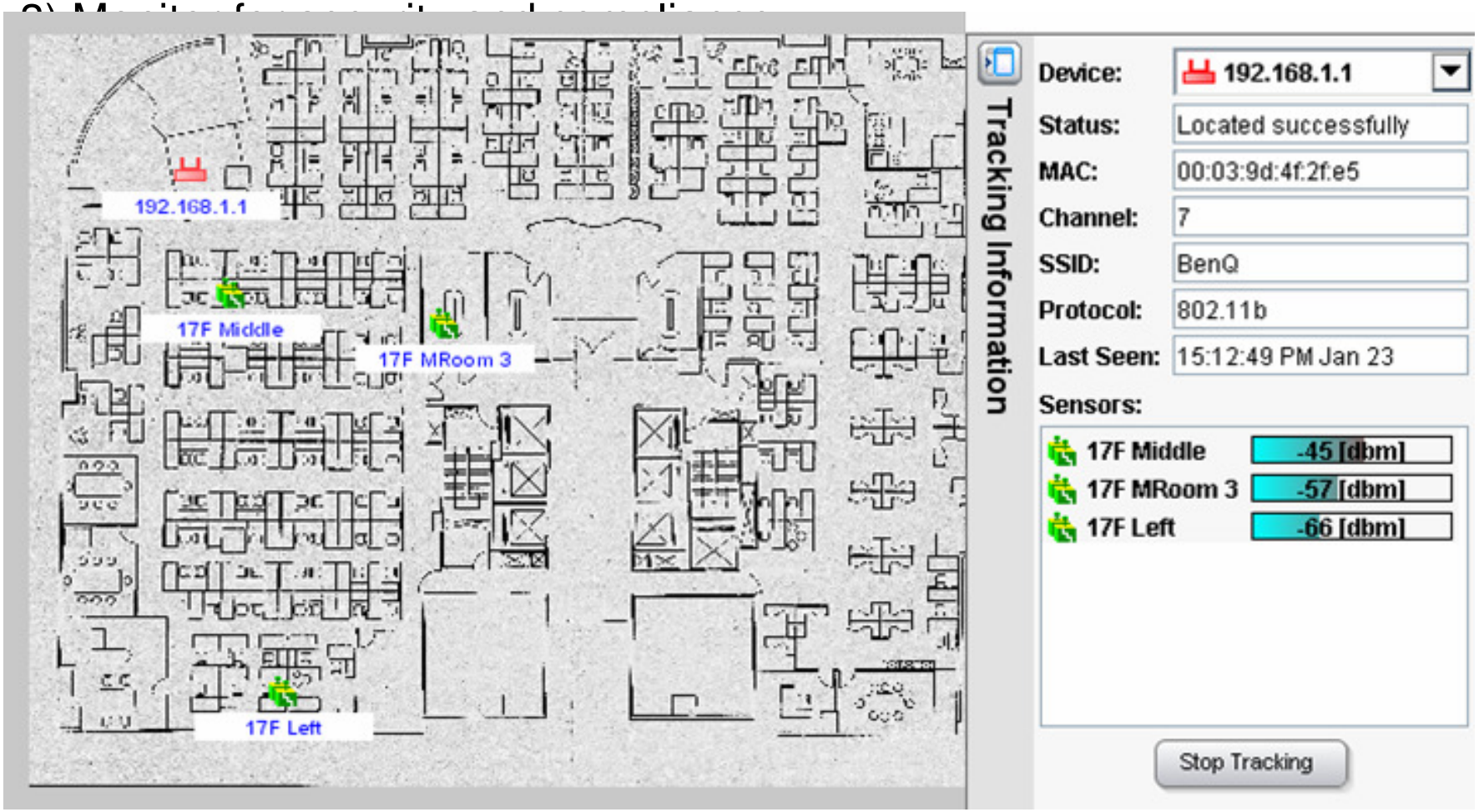
- Reconfigure from default settings (SSID, Admin login, Password etc.)
- Establish set Channels of operations – off channel traffic as suspicious activity

2) Secure Communications

- MAC address filtering
- WPA-2 encryption……and keep updates
- VPNs
- Personal Firewall
- End-point security

New Wireless Security Approach

Datacraft



Maintain Good Health – Wireless Assessment

Datacraft

Common Mis-concepts

- I do not deploy wireless networking
- I do not allow my users to use wireless

How can you be sure?

10 Steps on Wireless Assessment:

1) Review existing security policies
2) Review the system architecture and configurations.
3) Review operational support tools and procedures
4) Interview users
5) Verify configurations of wireless devices
6) Investigate physical installations of access points
7) Identify rogue access points
8) Perform penetration tests
9) Analyze security gaps
10) Recommend improvements

Maintain Good Health – Wireless Assessment

Datacraft

BackTrak

- Free suite
  - Snort
  - ntop
  - db_auto
  - kismet
  - unicorns
- No Installati
- What it can
  - Foot-pri
  - Analysis
  - Scannin
  - Wireless
  - Brute-fo
  - Crackin

References

PISA War Driving 2007

http://www.pisa.org.hk/event/war-driving-2007.htm

Network Stumbler

http://www.netstumbler.com/

The Café Latte Attack

http://www.airtightnetworks.net/knowledgecenter/ppt/Toorcon.ppt

AirDefense Network

http://www.airdefense.net

AirDefense Network

http://www.airdefense.net

Datacraft

End of Presentation