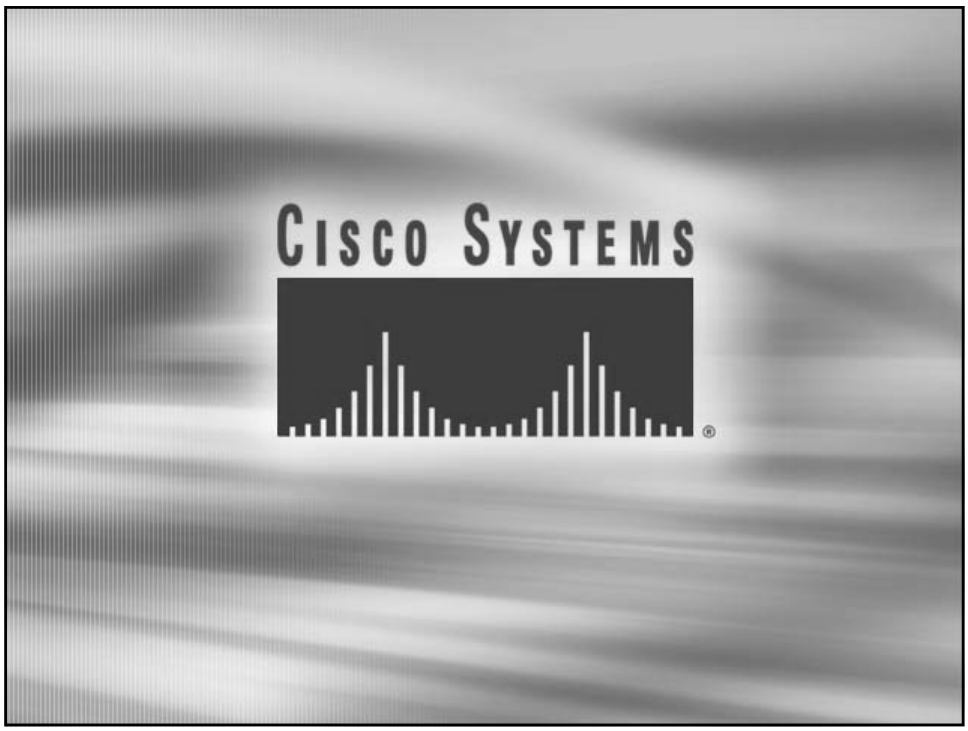


Cisco Systems

The CSIRT and Wireless Security Breaches

Lance Hayden & Marcus Sitzman

Cisco Advanced Services for Network Security

What Are we Talking About??

Cisco.com

- Proactive WLAN Security Measures (Acme Widgets)
- Threats to WLAN Security
- WLAN Security Breaches (Acme Widgets)
- Reactive Policies and Procedures

Proactive WLAN Security Measures

Acme Widgets Case Study

Hide Your Wireless Network

Cisco.com

- **Reduce Transmit Power**
  - **Creates a smaller range of the wireless signal**
- **Require Faster Connection Speeds**
  - **Smaller association circle**
- **Cloaked Service Set Identifier (SSID)**
  - **Not revealed in management frames**
- **Disable Broadcast Association**
  - **SSID must be known and configured**

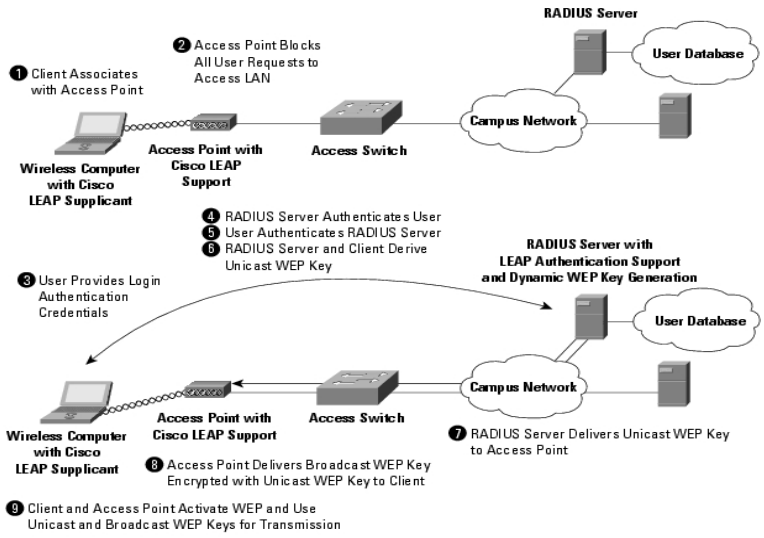
Register Your MAC Address

Cisco.com

- **Require users to register there WLAN adapters MAC address**
  - **Binds a client adapter to a user**
  - **Easy web page registration**
- **Utilize MAC address filters across AP devices**
  - **Identify DHCP scopes**
  - **Automated filter updates to APs**

User Authentication via LEAP

Cisco.com



CISCO SYSTEMS

Threats to WLAN Security

Tools and Methods

Rogue Access Points

Cisco.com

- **Connected by External Entity**
  - **Requires James Bond like practices**
  - **Deliberate security breach**
  - **Not very common**
- **Connected by Internal Entity**
  - **Independent department/employee actions**
  - **Intent is to increase productivity**
  - **Most common**

Watching the Airwaves

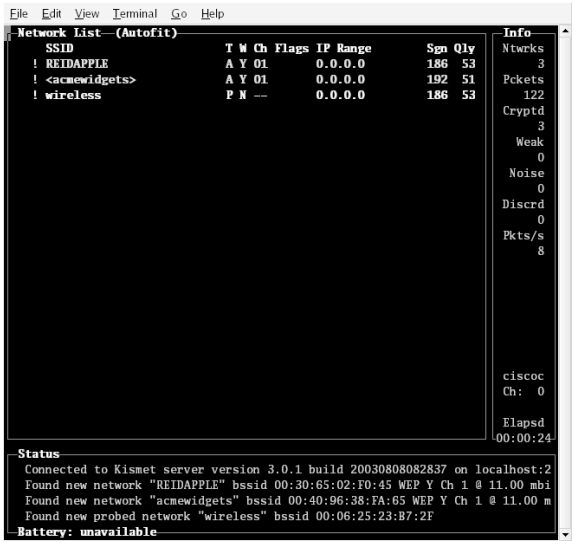
Cisco.com

- **Is someone in your company parking lot (or worse across the street)?**
  - **Wireless signal access depends largely on the client antenna**
  - **Usually trivial to track down a wireless network**
- **Offline data analysis of captured frames**

Kismet WLAN Sniffer

Cisco.com

- Network mapping
- WLAN configuration settings
- Packet dump in pcap format



How Strong is Your Encryption?

Cisco.com

- Many WLANs without any encryption
  - Often an indicator of a rogues access point
- Static WEP… obviously not going to work
  - Administration issues
  - 40 and 128 bit encryption keys will be cracked
  - WLAN clients that have limited support for security protocols

Are You Really You??

Cisco.com

- **MAC address filters**
  - **Forged MAC addresses**
    - **Client adapter utility**
    - **Unix/Linux capabilities**
- **User Authentication**
  - **Reconnaissance information**
  - **Cracked passwords**

CISCO SYSTEMS

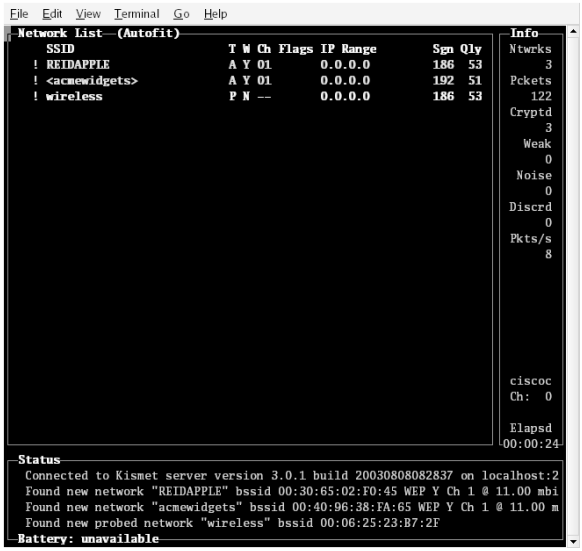
WLAN Security Breaches

Acme Widgets Case Study

Kismet WLAN Sniffer

Cisco.com

- Cloaked SSID
- Descriptive SSID
- Encrypted Network



MAC Address Forging

Cisco.com

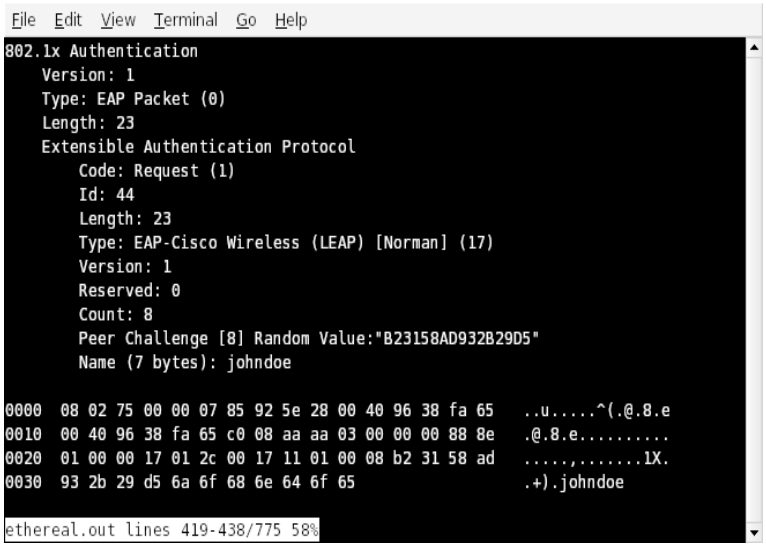
```
File  Edit  View  Terminal  Go  Help
[root@ghostrider authen]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:09:B7:7E:C5:13
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:14 dropped:0 overruns:0 frame:14
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100

[root@ghostrider authen]# ifconfig eth1 hw ether 00:07:85:92:5e:28
[root@ghostrider authen]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:07:85:92:5E:28
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:22 dropped:0 overruns:0 frame:22
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:3 Base address:0x100

[root@ghostrider authen]#
```

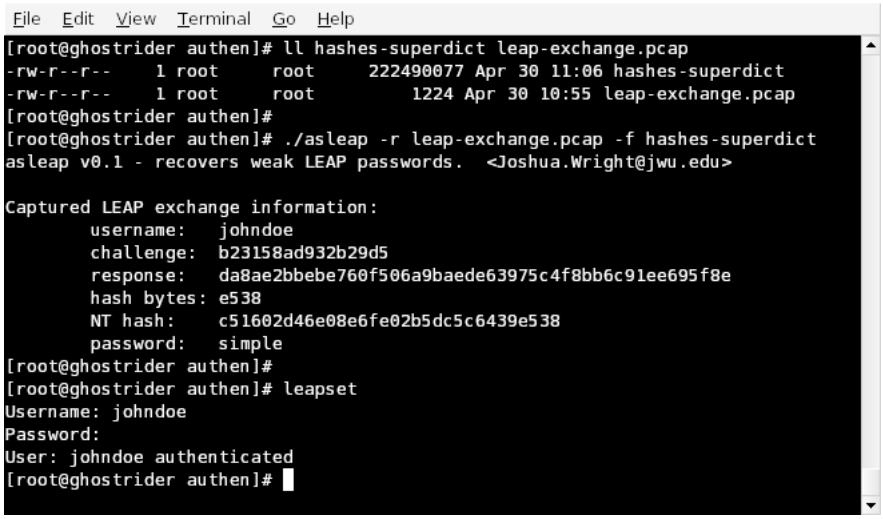
LEAP User Authentication

Cisco.com



Cracked User Credentials

Cisco.com



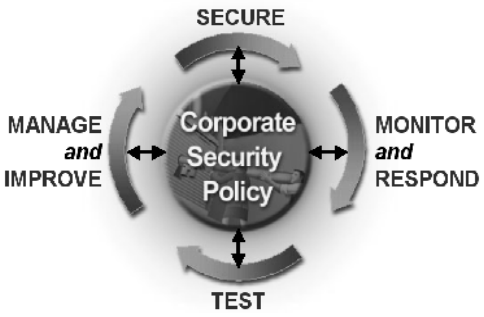
Cisco Systems

Policies and Procedures

Specialized Tools and CSIRT Plug-in

Security Practices

- **WLAN security is continually evolving**
- **Security teams using a process-based model will be most successful**



Intrusion Detection

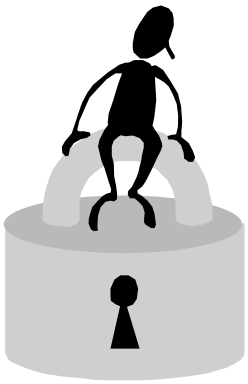
Cisco.com

- **Rogue AP Detection**
  - **Listen for wireless frames from unauthorized APs (not effective by itself)**
  - **Search internal MAC tables for identified BSSIDs (most effective)**
    - **Proof of concept tool: mac-find.py**
- **Identify Known Wireless Tools**
  - **Detectable signatures of tools**

Points for WLAN Security

Cisco.com

- **Defense in depth approach to security**
- **Design the right solution**
- **Risk assessment analysis**
- **Policies for WLANs**
- **Procedures for security breaches**
- **Implement incident detection solution**

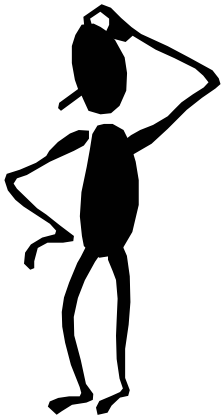


Wrap-up

Cisco.com

Questions… discussion…

- **Lance and Marcus available after the presentation**



CISCO SYSTEMS

Contact Info

Lance Hayden, Program Strategy Manager
lhayden@cisco.com 512.378.1072

Marcus Sitzman, Network Security Engineer
msitzman@cisco.com 408.525.2999