SANS Institute presents:

Four Ways To Monitor Your Wireless Network

Today's Speakers

- Joshua Wright, SANS Institute
- Bryan Wargo, AirWave
- Q/A session with today's speakers
- Send questions to 'q@sans.org'

Wi-Fi Monitoring Made Easy

Bryan Wargo
VP Sales & Business Development
Bryan.Wargo@AirWave.com
650-286-6103

AirWave Overview

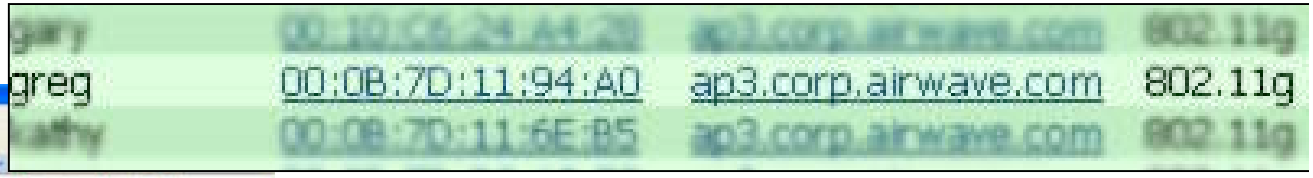
Security	Management
"If Wi-Fi isn't managed, it's not secure"	**"One console does it all"**
• Policy definition & enforcement	• End-to-end management
• Automated audit & compliance	• Discovery & provisioning
• Enforce access control policies	• Configuration & firmware Management
• Rogue AP detection & elimination	• Monitoring, diagnostics & reporting
Visibility	**WiFi ROI**
"Nothing's invisible – not even the air"	**"Make wireless pay"**
• See everything that is happening	• Fewer network problems
• Visualize the RF airspace	• 75% faster troubleshooting
• Know who, what and WHERE	• Usable by the entire staff
• Real-time health-check of the network	• Capacity planning and reporting

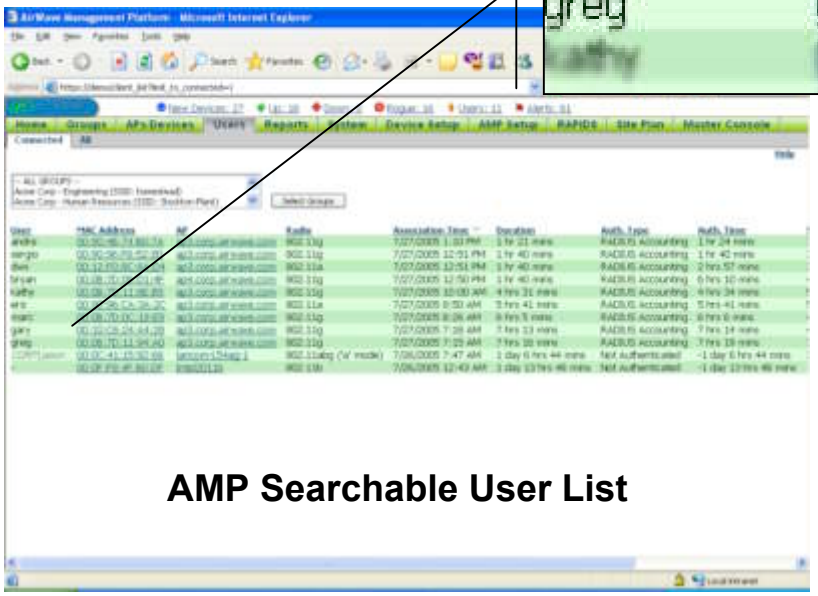
Key Wireless Issues

- Monitoring must be both *real-time* and *automated*
- For scalability, solution must be easy enough for your Help Desk to use
- Everything must be VISIBLE – you cannot manage what you cannot see
- If the WLAN is not managed, it's not secure

User-based Monitoring

- User "greg" complains that of a slow connection
- Help Desk uses AMP to locate the "greg" on the WLAN *by username:*

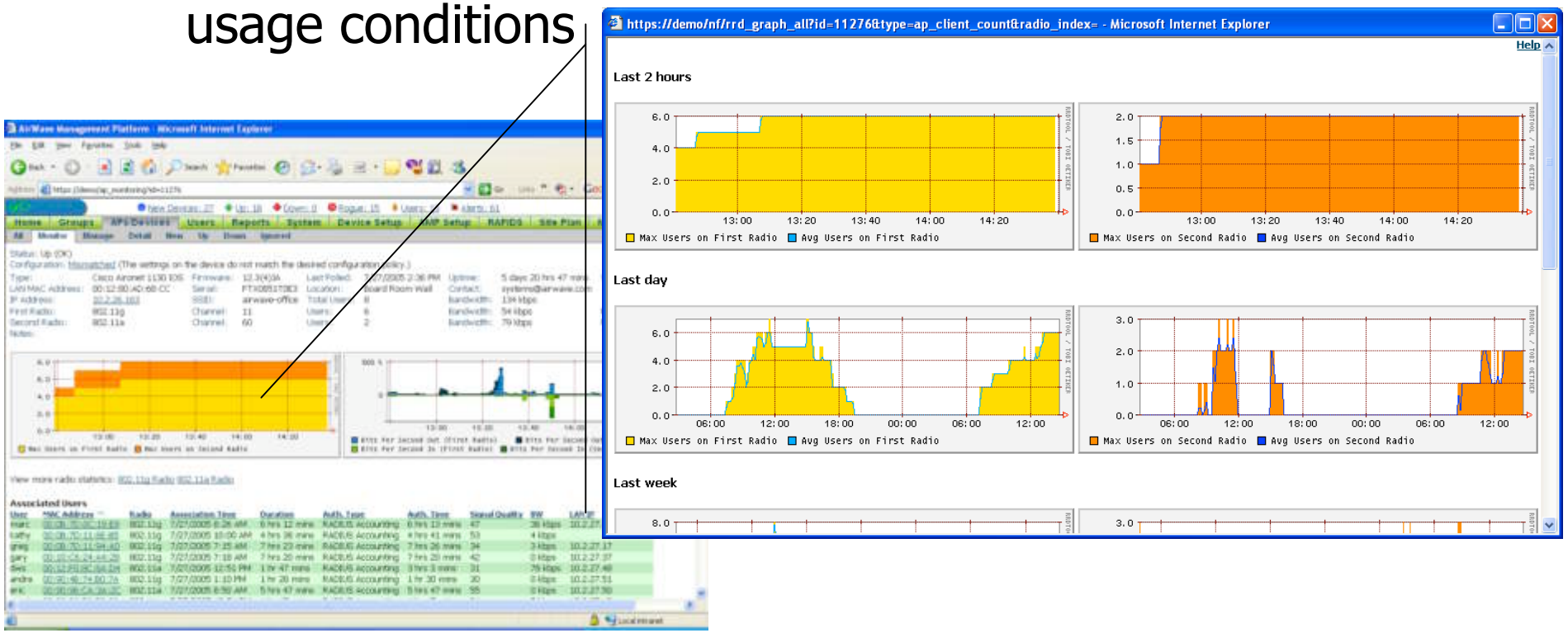




AMP Searchable User List

AP-level Drill Down

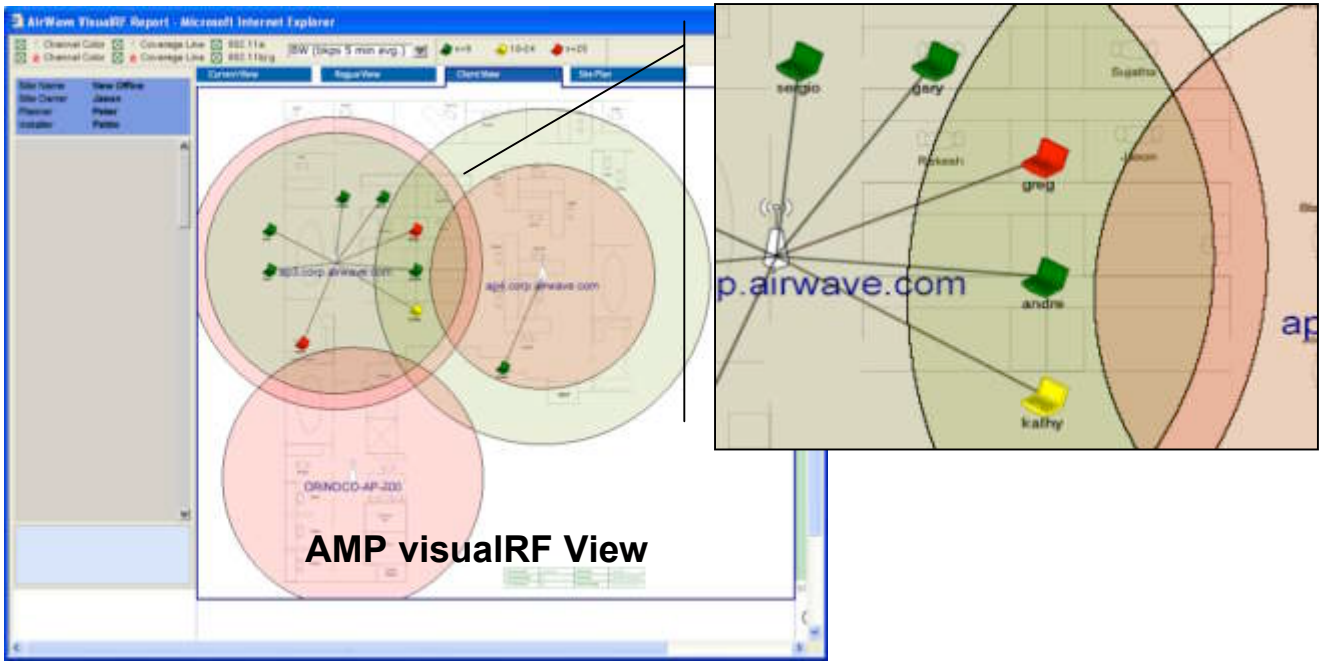
- Help Desk drills into "AP View", examining current usage conditions



Real-time AP Monitoring Screen

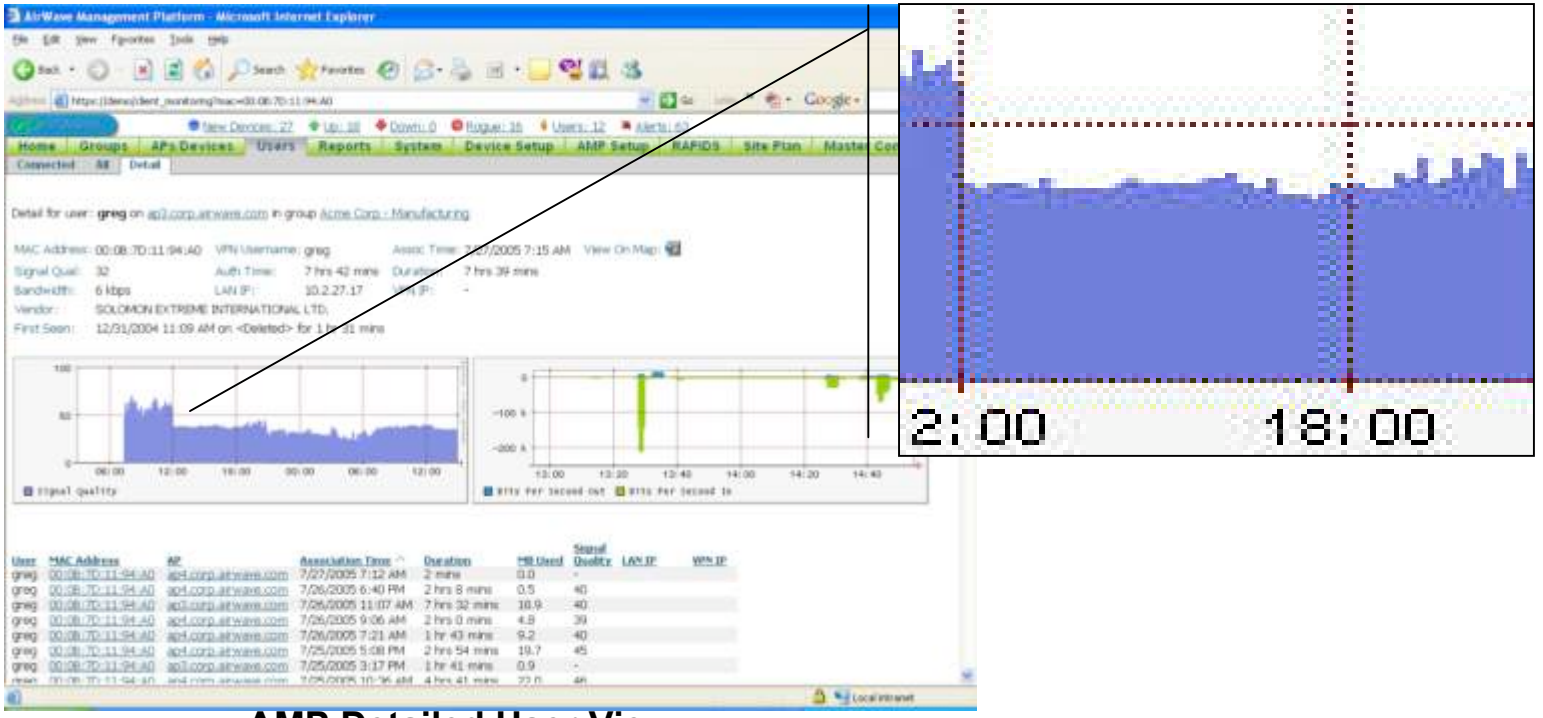
Wi-Fi Visualization

- Help Desk toggles to AMP's visualRF™ view to assess real-time RF and usage conditions in the area



Real-time RF Diagnostics

- Help Desk drills into detailed "User View" to see real-time and historical data for user "greg," noting steep drop in RF signal strength



AMP Detailed User View

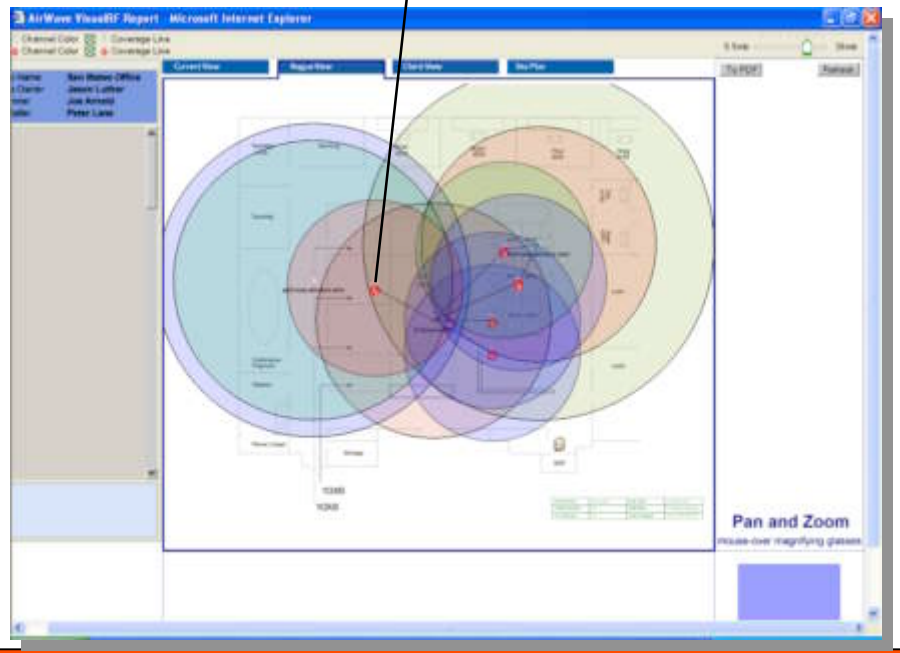
Configuration Monitoring

- Manual configuration audits simply do not get done
- AMP automatically audits each AP on your network
- Alert & "auto-repair" when any configuration violations are detected

Rogue Detection & Monitoring

- RAPIDS scans the wired network to detect unknown APs
- Uses existing APs to conduct wireless RF scans
- Correlates data to locate rogues in physical space

Name:	3Com Rogue AP	Type:	-
Radio MAC Address:	00:0A:5E:08:A5:7B	IP Address:	10.51.3.3
Radio Vendor:	3COM	SSID:	3comradio
LAN MAC Address:	00:0A:5E:08:A5:7B	Channel:	1
LAN Vendor:	3COM	WEP:	No
Current Score:	5	Network Type:	AP
OUI Score:	3		



Monitoring Value Proposition

- AirWave will **SAVE YOU MONEY** by reducing the cost of operating your wireless network
- AirWave will **MAKE YOUR NETWORK MORE SECURE** by automatically enforcing security policies and auditing your infrastructure
- AirWave will **KEEP YOUR USERS HAPPY** by improving the performance of your network
- AirWave will **FUTURE-PROOF YOUR NETWORK** by supporting leading hardware vendors and all industry standards

AirWave's Customers

Special Offer for SANS

- Email sales@airwave.com or call 866.802.1121
- Mention "SANS" and receive a 30-day evaluation copy of the AirWave Management Platform at no cost

Bryan Wargo
VP Sales & Business Development
Bryan.Wargo@AirWave.com
650-286-6103

Four Ways to Monitor Your Wireless Network

Joshua Wright
SANS Institute
jwright@sans.org

Start sending questions to "q@sans.org"

The Need to Monitor Wireless

- "The network perimeter is dead"
- Centralized monitoring mechanisms often unhelpful at network edge
- Wireless networks expanding, growing at an alarming rate
  - Netgear ME102 802.11b AP - $16
- Wireless attacks can be subtle

Webcast Focus

- Four techniques for monitoring wireless networks
- Leveraging open-source/free tools
- Some tools are Linux-only
- Commercial tools simplify monitoring, come with support!

Change Management

- Unplanned downtime often due to misconfiguration issues
- Monitor AP for signs of unauthorized change
  - IT staff not following change mgmt.
  - Adversary that has compromised AP
- Assess config. regularly, report changes

Subtle Configuration Issue

```
interface Dot11Radio0
 encryption mode ciphers wep128 tkip
 !
 encryption vlan 101 ciphers tkip
 encryption vlan 102 ciphers tkip
 !
 ssid petnet101
    vlan 101
    authentication network-eap eap_methods
 !
 ssid petnet102
    authentication network-eap eap_methods
```

What encryption mechanism is used for "petnet102"?

Change Monitoring Goals

1. Identify unauthorized changes to configuration
2. Alert administrators to changes
   - Careful not to transmit sensitive info.
3. Save changes to revert to previous configuration when troubleshooting
4. Automate configuration restoration following unauthorized change

RANCID

"Really Awesome New Cisco confIg Differ"

- Open-source tool for Linux, Unix systems
- Supports IOS, CatOS, JunOS, others
- Grabs configuration file, compares to previous capture
  - Sends *diff* output to administrator
  - Stores new configuration in CVS repository
- Automate by running with cron

http://www.shrubbery.net/rancid/

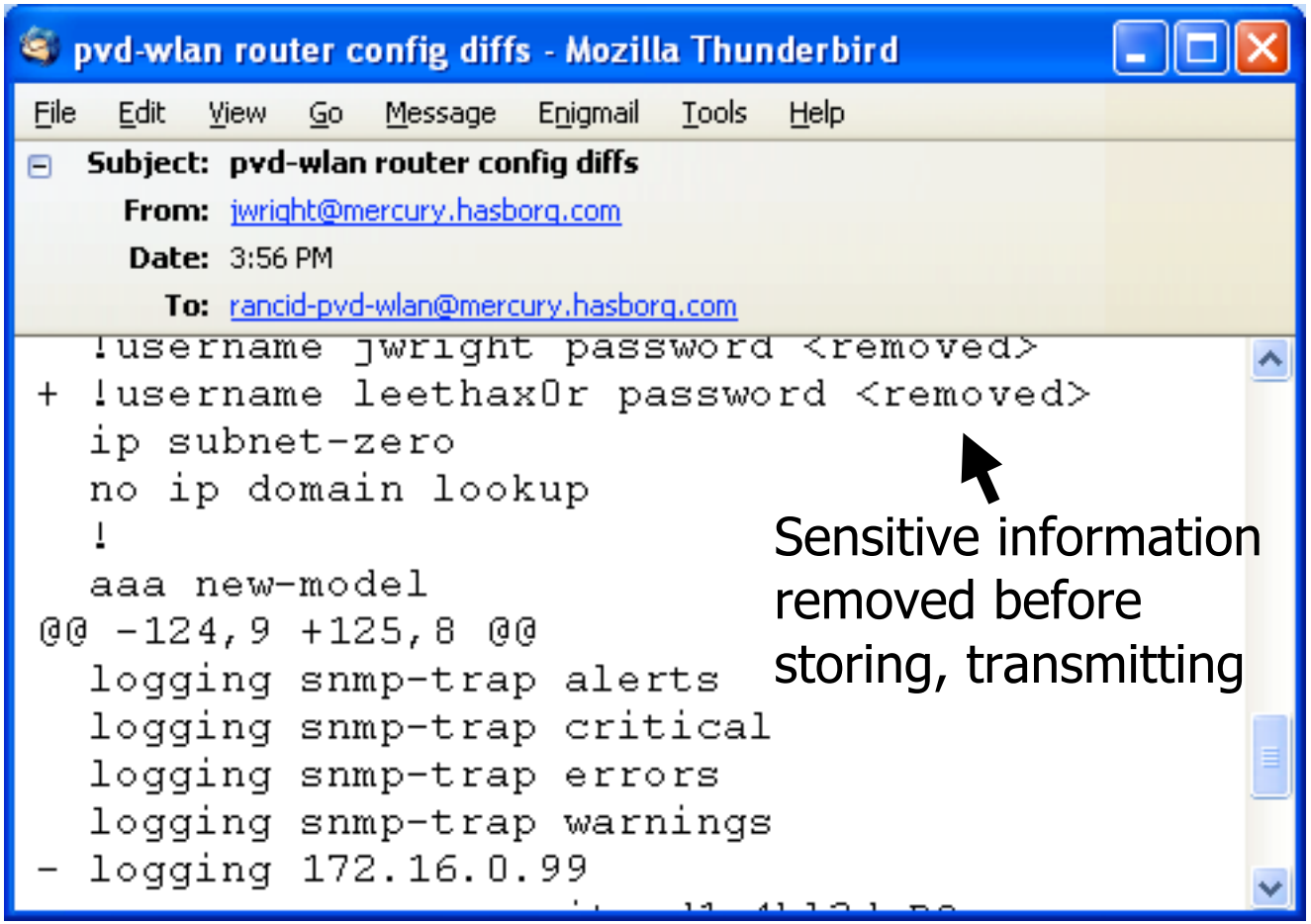
Installing RANCID

- "Easy" 12-step installation
  - Unix skills needed here!
- RANCID needs Expect, TCL, Perl, CVS and GNU diff installed
- Follow install instructions in README
  - Edit router.db "ap-address-host:cisco:up"
  - Supply login name and pass in ~/.cloginrc
- Run "rancid-run" until logs in $BASE/rancid/var/logs are error-free

RANCID Results

New entries are prefixed with "+"

Removed lined are prefixed with "-"



Sensitive information removed before storing, transmitting

Retrieving Historical Configs

- CVS can reproduce configuration from any previously gathered date
- Stores changes, little disk needed
- Must manually restore sensitive data (passwords, shared secrets, keys)

```
$ CVSROOT=/usr/local/rancid/var/CVS
$ cvs co -D "last friday" pvd-wlan
cvs checkout: Updating pvd-wlan
cvs checkout: Updating pvd-wlan/configs
$ more pvd-wlan/configs/172.16.0.94
```

Utilization Monitoring

- SNMP MIBs provide a wealth of information about AP
  - Utilization/throughput on interfaces
  - Number of connected users
  - Retransmitted packets, errored packets
- Establish standard data collection, graph
- Use data to identify network anomalies

MRTG

- Multi-Router Traffic Grapher
- Collects SNMP statistics, generates graphs at 5 minute intervals
- More sophisticated collection exists (Cricket), but not for Windows+Unix

www.mrtg.org

Installing MRTG

- Requires Perl, Windows users can download from activestate.com
- Schedule to run every 5 minutes, or specify "RunAsDaemon"
  - Windows users can run as a service with FireDaemon
  - www.firedaemon.com/HOWTO/MRTG/
- No automated tools to configure wireless statistical data collection

SNMP OID

- SNMP Object Identifiers specify data location within SNMP MIB
- 802.11 MIBS provide useful data
- Can also extract from vendor-proprietary MIB data
- Edit mrtg.cfg to specify OID, options for collection

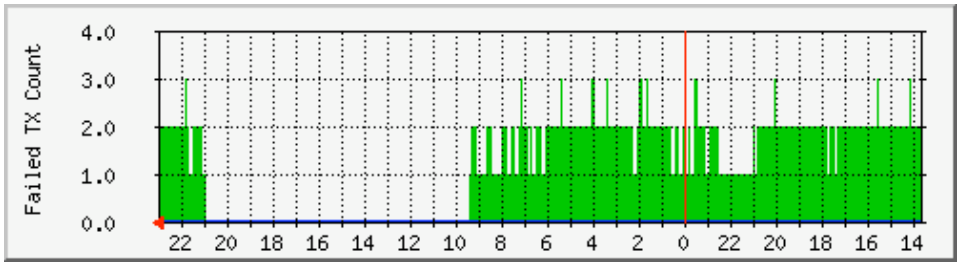
```
$ snmpget -c public 172.16.0.92 .1.2.840.10036.2.2.1.3.1
iso.2.840.10036.2.2.1.3.1 = Counter32: 94119
```

802.11 OID Data

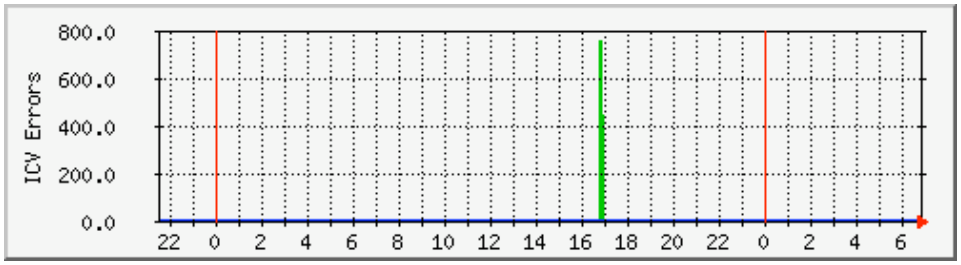
- dot11FailedCount - excessive retries on network
  - Interference, or potential DoS attack
- dot11WEPICVErrorCount - bad ICVs observed on WEP network
  - Characteristic of "chopchop" attack
- dot11ReceivedFragmentCount - number of fragmented packets received
  - Characteristic of 802.11 fragment attack
- Cisco proprietary MIB - # of connect users

MRTG Graphs

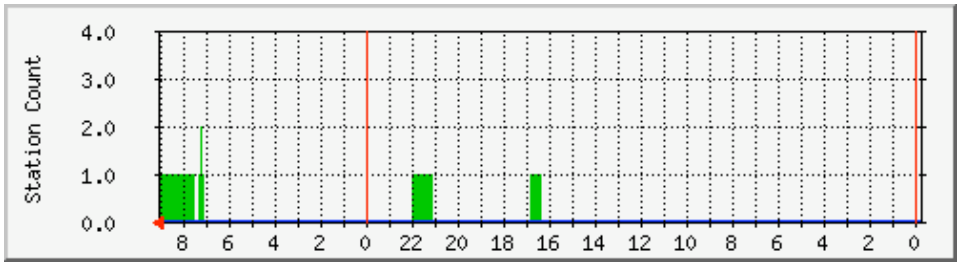
Failed TX



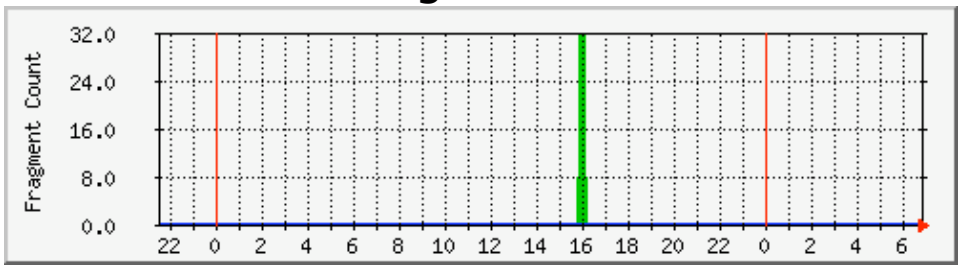
ICV Errors



Number of Users



Fragment Count



Sample mrtg.cfg, tested with Cisco IOS at
http://files.sans.org/webcasts/20051005/mrtg.cfg

Logging Messages

- Many AP's generate logging data that can help identify misuse
- Aggregate logging data in a central repository over Syslog
  - Examine data for anomalies with Swatch, Unix/Linux only
  - Can use custom Perl/VBScript for Windows
- Identify failed authentication attempts, invalid packets, attacks against AP

Installing Swatch

- Download Swatch from swatch.sf.net
- Requires Perl and CPAN modules

```
# tar xfz swatch-3.1.1.tar.gz
# cd swatch-3.1.1
# perl -MCPAN -e 'install Date::Calc'
# perl -MCPAN -e 'install Date::Parse'
# perl -MCPAN -e 'install Date::Manip'
# perl Makefile.PL
# make && make install
# swatch --version
This is swatch version 3.1.1
Built on 19 Jul 2004
Built by E. Todd Atkins <Todd.Atkins@StanfordAlumni.ORG>
```

Sample Swatch Config File

```
$ cat $HOME/.swatchrc
# Error in 802.11 association state table, could represent
# malicious traffic attacking AP
watchfor /DOT11-3-BADSTATE/
# STAs with Cisco client drivers can report rogue AP's
watchfor /DOT11-6-ROGUE_AP/
# Unexpected error conditions indicate an IOS bug or an attack
# against the AP (such as a buffer-overflow attack)
watchfor /SCHED-3-UNEXPECTED/
# A station has failed 802.1x authentication
watchfor /DOT11-AUTH_FAILED/
# TKIP errors seldom happen with regular use, are usually an
# indicator of an attack against TKIP to cause a DoS attack
watchfor /DOT11-TKIP_MIC_FAILURE/
      mail=admin@xyz.org,subject=Aironet Logging Alert Message
```

Running Swatch

- Direct all logging data for AP's to one log file
- Create swatchrc file with watchfor statements, actions
- Test Swatch, then run in background

```
$ swatch --examine /var/log/aironet-aggregated
*** swatch version 3.1.1 (pid:29007) started at Thu Sep 15
14:10:16 EDT
$ swatch --tail-file /var/log/aironet-aggregated &
[1] 29022
```

Swatch Logging Alert

Wireless Traffic Capture

- Wireless-side monitoring provides comprehensive data for analysis
- Provides lots of data, requires protocol understanding
- Typically requires local access

How can we get detailed wireless analysis data that can be assessed centrally (using free/inexpensive tools)?

Kismet

www.kismetwireless.net

- Wonderfully powerful wireless analysis tool (Mike Kershaw)
- Written for Linux/BSD systems
  - Not ported to Windows due to lack of native 802.11 packet capture support
- Client-server architecture, includes lightweight capture engine (drone)
- Drone can run on Linksys WRT54G

Linksys WRT54G

- Common, inexpensive SOHO AP
- Runs Linux! Alternate firmware available from openwrt.org (~$50)
- Re-flash AP into general-purpose Linux device
- Load kismet_drone to capture traffic
- Use locally or send to remote locations

Running Kismet on WRT54G (1)

- Download new firmware
  - downloads.openwrt.org/whiterussian/rc2/bin/openwrt-wrt54g-squashfs.bin
- Upgrade WRT with firmware
  - May void warranty!
- Telnet to WRT to access root prompt
- Change password with "passwd", then logout and login over SSH
  - Then change password again!

Running Kismet on WRT54G (2)

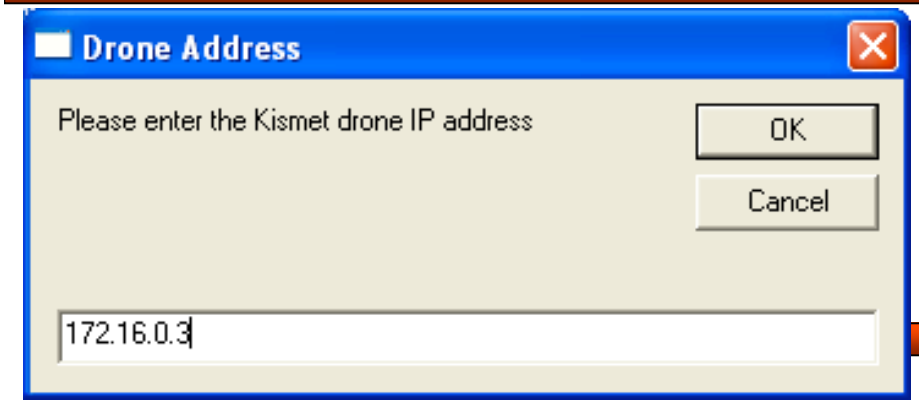
```
# echo 'nameserver 10.10.10.10' >/etc/resolv.conf
# route add default gw 10.10.10.1
# ipkg update
# ipkg install kismet-drone wl
# vi /etc/kismet/kismet_drone.conf
                        Edit as shown:
source=wrt54g,eth1:prism0,wrt54g
allowedhosts=127.0.0.1,10.10.10.0/24

# wget http://files.sans.org/webcasts/20051005/wrt-files.tar
-O /wrt-files.tar
# cd / ; tar xf wrt-files.tar ; rm wrt-files.tar
# chmod 755 /etc/init.d/S60* /etc/init.d/S70*
/usr/bin/kismet_hopper.sh
# reboot
```

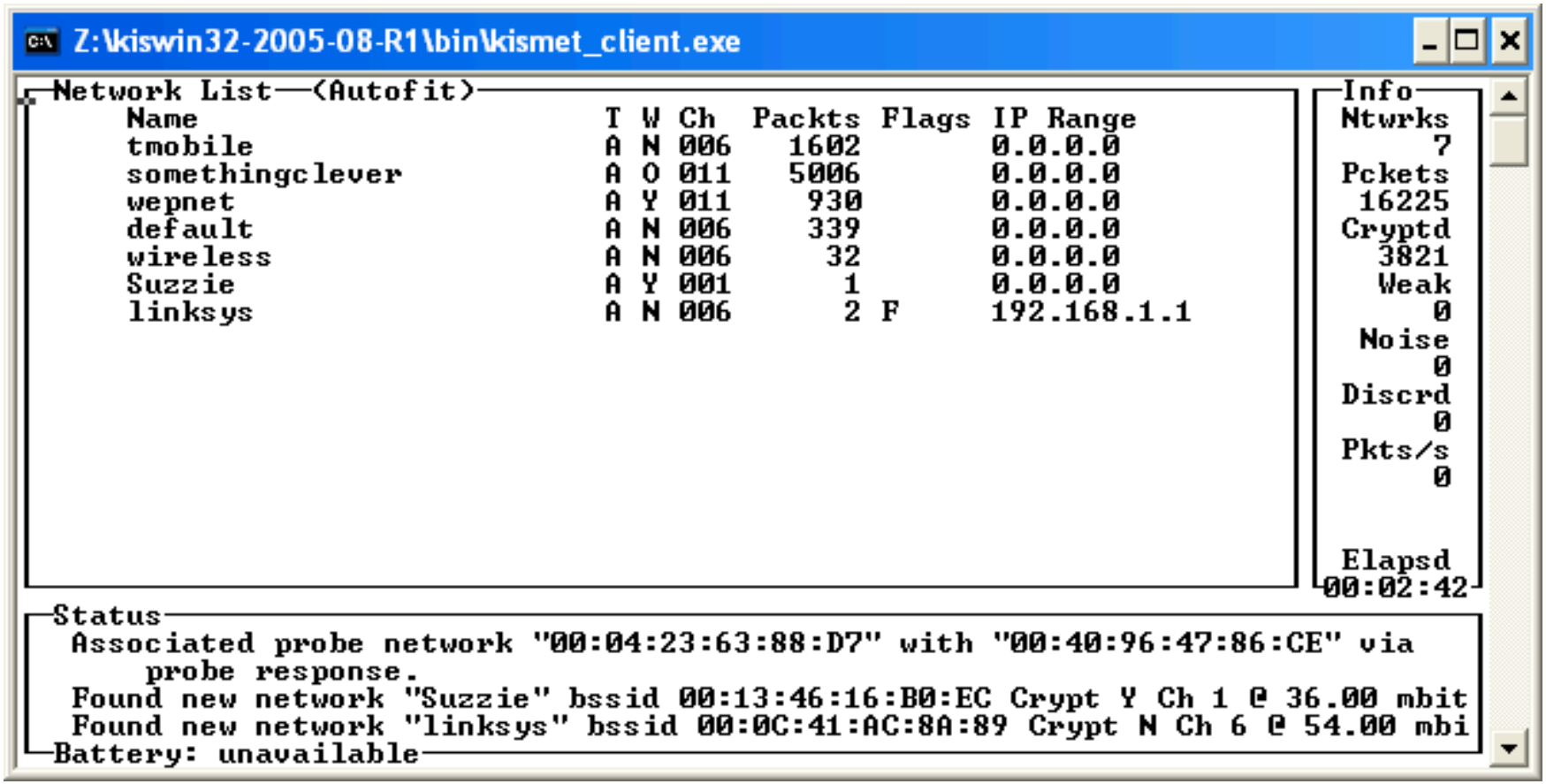
Kismet for Windows

- Compiled Kismet code using Cygwin
- Tested with WinXP SP2
- Download kiswin32 zip file, extract to local directory
  - Extract terminfo.zip to %HOMEPATH%
- Double-click "kiswin32.vbs"
- Unsigned code, will generate warning

http://files.sans.org/webcasts/20051005/kiswin32-2005-08-R1.zip

kiswin32


Drone Address
Please enter the Kismet drone IP address
OK
Cancel
172.16.0.3


Z:\kiswin32-2005-08-R1\bin\kismet_client.exe
Network List—(Autofit)
Name T W Ch Packts Flags IP Range
tmobile A N 006 1602 0.0.0.0
somethingclever A O 011 5006 0.0.0.0
wepnet A Y 011 930 0.0.0.0
default A N 006 339 0.0.0.0
wireless A N 006 32 0.0.0.0
Suzzie A Y 001 1 0.0.0.0
linksys A N 006 2 F 192.168.1.1
Info
Ntwrks 7
Pckets 16225
Cryptd 3821
Weak 0
Noise 0
Discrd 0
Pkts/s 0
Elapsd 00:02:42
Status
Associated probe network "00:04:23:63:88:D7" with "00:40:96:47:86:CE" via probe response.
Found new network "Suzzie" bssid 00:13:46:16:B0:EC Crypt Y Ch 1 @ 36.00 mbit
Found new network "linksys" bssid 00:0C:41:AC:8A:89 Crypt N Ch 6 @ 54.00 mbi
Battery: unavailable

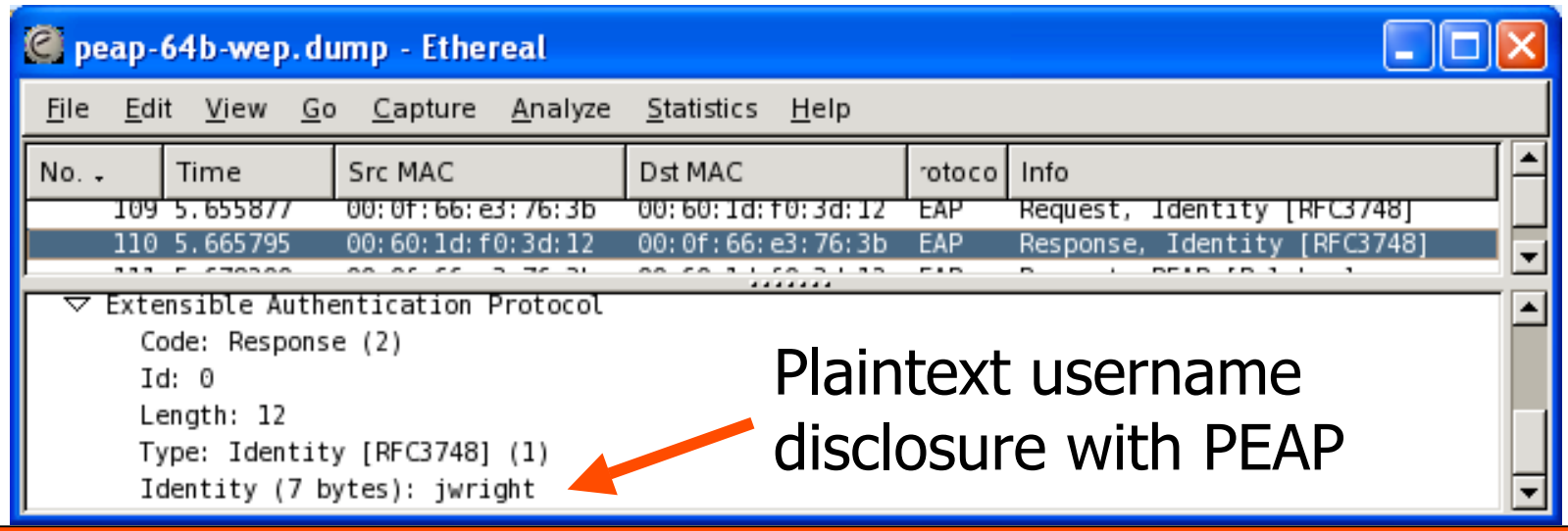
Monitoring with Kismet

- WRT collects wireless packets, transmits them to the Kismet server
- Lots of great uses:

_ Identifying rogue threats
_ Wireless network monitoring
_ Identifying plaintext information disclosure
_ WLAN IDS
_ Identifying nearby networks for optimum channel selection
_ Wardriving
_ Enumerating clients

Assessing with Ethereal

- Ethereal augments Kismet for post-capture analysis
  - Opens Kismet ".dump" files



Summary

- 90% of users leverage 10% of features
- Existing wireless AP's can provide more detailed information
  - Helpful for security and operational/troubleshooting issues
- Change management, SNMP MIB data, logging records, traffic collection
- Select the tools that best suit your needs

Questions?

- Email your questions to q@sans.org
- We'll answer as many as time allows!
- Thank you for attending!

Joshua Wright - jwright@sans.org