Hacking Exposed 7
Network Security Secrets & Solutions

Chapter 8 Wireless Hacking

AIRCRACK-NG

Home
Forum
Wiki
GitHub
Blog
IRC

Documentation

Getting started
Installation
Compatibility
Screenshots
In movies
Main Docs

Misc

Support
Resources
Contribute
Contact
License
Code of Conduct

Download

- Aircrack-ng 1.2
  - Sources
  - Windows
- Changelog

More downloads...

Description

Aircrack-ng is a complete suite of to

It focuses on different areas of WiFi

- Monitoring: Packet capture and e processing by third party tools.
- Attacking: Replay attacks, deauth others via packet injection.
- Testing: Checking WiFi cards and injection).
- Cracking: WEP and WPA PSK (WP

All tools are command line which allo have taken advantage of this feature Windows, OS X, FreeBSD, OpenBSD, eComStation 2.

Fresh news

Aircrack-ng 1.2 15 Apr 18

It's been way too long since the last stable release.

Compared to the last stable, 1.1, this release has a huge amount of improvements and fixes. The changelog since 1.1 is almost 300 lines long (1200+ commits). Code quality has improved, in parts thanks to

Under the spotlights

Injection, -1 channel and other ca

If you are having issues injecting or message talking about channel -1 o right of the screen) or aireplay-ng, `airmon-ng check kill` before putting the

Case Study on Wireless Hacking Read It and WEP (not Weep)

- A store with the point-of-sale system connected through Wi-Fi /w WEP (Wired Equivalent Privacy) encryption
- A hacker at the parking lot turns laptop with Wi-Fi card and directional antenna to promiscuous mode
- aircrack-ng
  - airodump-ng to sniff 802.11 frames including WEP initialization vectors (IVs)
  - Look for SSID (service set identifier) of interest and its MAC address
  - aireplay-ng to spoof as a client to capture ARP and replay it to collect enough IVs
  - aircrack-ng to crack WEP key from the capture file
  - Disable the promiscuous mode
  - Enter WEP key and get an IP address from the DHCP server

Background on IEEE 802.11 Wireless LAN

- Frequencies and channels
  - ISM (Industrial, Scientific, Medical) unlicensed bands
  - 2.4 GHz: 802.11b/g/n, channels 1-14, non-overlapping channels: 1, 6, 11
  - 5 GHz: 802.11a/n, channels 36-165, all non-overlapping

Session Establishment

Infrastructure v. Ad Hoc

- Infrastructure
  - Uses an access point
  - Most common mode
- Ad Hoc
  - Devices connect peer-to-peer
  - Like an Ethernet crossover cable

Probes

- Client sends a **probe request** for the **SSID (Service Set Identifier)** it is looking for
- It repeats this request on every channel, looking for a **probe response**
- After the response, client sends **authentication request**

Authentication

- If system uses **open authentication**, the AP accepts any connection
- The alternate system, **shared-key authentication**, is almost never used
  - Used only with WEP
- WPA security mechanisms have no effect on authentication—they take effect later

Association

- Client sends an **association request**
- AP sends an **association response**

Security Mechanisms

Basic Security Mechanisms

- MAC filtering
- "Hidden" networks
  - Omit SSID from beacons
  - Microsoft recommends announcing your SSID because Vista and later versions of Windows look for beacons before connecting
  - This makes client more secure, because it is not continuously sending out probe requests, opening up to AP impersonation attacks

Mind your probes: De-anonymization of large crowds through smartphone WiFi probe requests

3
Author(s)

Adriano Di Luzio ; Alessandro Mei ; Julinda Stefa

View All

Abstract:
Whenever our smartphones have their WiFi radio interface on, they periodically try to connect to known wireless APs (networks the us
connected to in the past). This is done through WiFi Probe requests - special wireless frames that contain the MAC address of the ser
and, in most of the cases, the human-readable name-string (SSID) of the known AP. This semantic information, inherent to the networ
sent in the clear and, if sniffed, can help discover important information and phenomena of people and human nature that have nothin
technology. In this paper we present the idea of exploiting WiFi probe requests to de-anonymize the origin of participants in large even
use of several, publicly available datasets containing more than 11M of probe requests collected in scenarios that are of citywide, nati
political meetings), and international religion-related relevance. We show how, by exploiting the semantic information brought by the re
probes, we are able to discover with high accuracy the provenance of the crowds in each event. In particular, the de-anonymization ou
two political meetings held few days before the election days in Italy match surprisingly well the official voting results reported for the t
parties.

Published in: INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications, IEEE

Responding to Broadcast Probe Requests

- Clients can send **broadcast probe requests**
- Do not specify SSID
- APs can be configured to ignore them

WPA v. WPA2/3

- 802.11i specifies encryption standards
- WPA implements only part of 802.11i
  - TKIP (Temporal Key Integrity Protocol)
- WPA2/3 implements both
  - TKIP
  - AES (Advanced Encryption Standard)

WPA Personal vs WPA-Enterprise

- One password applies to all users
- Password is stored on the wireless clients
- Password manually changed on all the wireless clients, once it's modified on the AP
- Wireless access cannot be individually managed

WPA Personal vs WPA-Enterprise

- When users try to connect to Wi-Fi, they need to present their enterprise login credentials.
- Users never deal with the actual encryption keys.
- Attackers cannot get the network key from clients.
- Offers individualized control over access to a Wi-Fi network

WPA PSK vs. 802.1x

- WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)
  - Uses Pre-Shared Key
- WPA-Enterprise 802.1x
  - Uses 802.1x and a RADIUS server
  - EAP (Extensible Authentication Protocol), which may be one of
    - EAP-TTLS
    - PEAP
    - EAP-FAST

Four-Way Handshake

- Both WPA-PSK and WPA Enterprise use Four-way handshake to establish:
  - Pairwise transient key (PTK)
    - Used for unicast communication
  - Group temporal key (GTK)
    - Used for multicast and broadcast communication

The 4-way handshake involves (PTK):

- The AP sending a random number (ANonce) to the client.
- The client responding with its random number (SNonce).
- The AP calculating the PTK from these numbers and sending an encrypted message to the client.
- The client decrypting this message with the PTK.

Three Encryption Options

- WEP (Wired Equivalent Privacy)
  - Uses RC4
  - Flawed & easily exploited
- TKIP
  - A quick replacement for WEP
  - Runs on old hardware
  - Still uses RC4
  - No major vulnerabilities are known
- Advanced Encryption Standard (Most secure, recommended)
  - CCMP (with Cipher Block Chaining Message Authentication Code Protocol) – WPA2
  - GCM (with Galois/Counter Mode with SHA-384 as HMAC) – WPA3

Equipment

Chipset

- Manufacturer's chipset driver limits your control of the wireless NIC
  - Most NICs can't be used for wireless hacking
- Recommended Network Cards
  - Ubuiquiti SRC, Atheros chipset, USB
  - Alfa AWUS050NH, Ralink RT2770F chipset, USB
  - Both support 802.11a/b/g/n and external antennas

  Band: 2.4 GHz and 5 GHz

Windows x. Linux

- Windows
  - Wireless NIC drivers are easy to get
  - Wireless hacking tools are few and weak
    - Unless you pay for AirPcap devices or OmniPeek
- Linux
  - Wireless NIC drivers are hard to get and install
  - Wireless hacking tools are much better

Kali

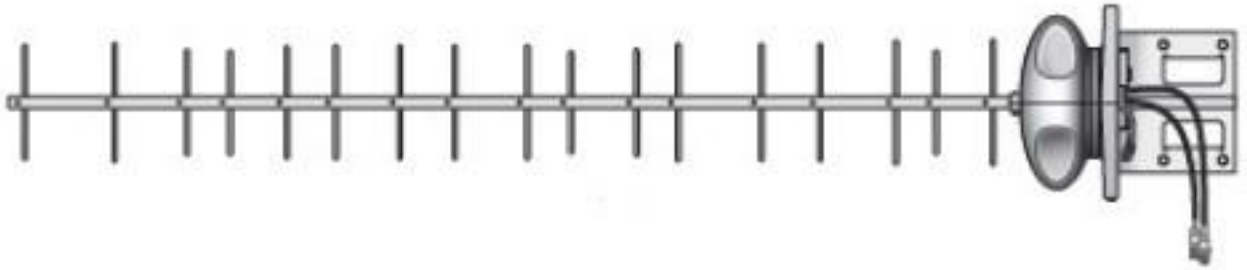
- Includes many drivers already ☺
- Can be used from a virtual machine with a USB NIC
- For other NIC types, you can't use VMware for wireless hacking
  - Install Kali on the bare metal
  - Boot from a USB with Kali on it
  - Boot from a LiveCD of Kali

Antennas

- Omnidirectional antenna sends and receives in all directions
- Directional antennas focus the waves in one direction
  - The Cantenna shown is a directional antenna

https://www.wikihow.com/Make-a-Cantenna

Yagi



Ubiquiti AMY-9M16 900MHZ Yagi Antenna Dual-Pol 16DBI (AMY-9M16)

Model: AMY-9M16

Availability: Usually Ships 7-12 Business Days

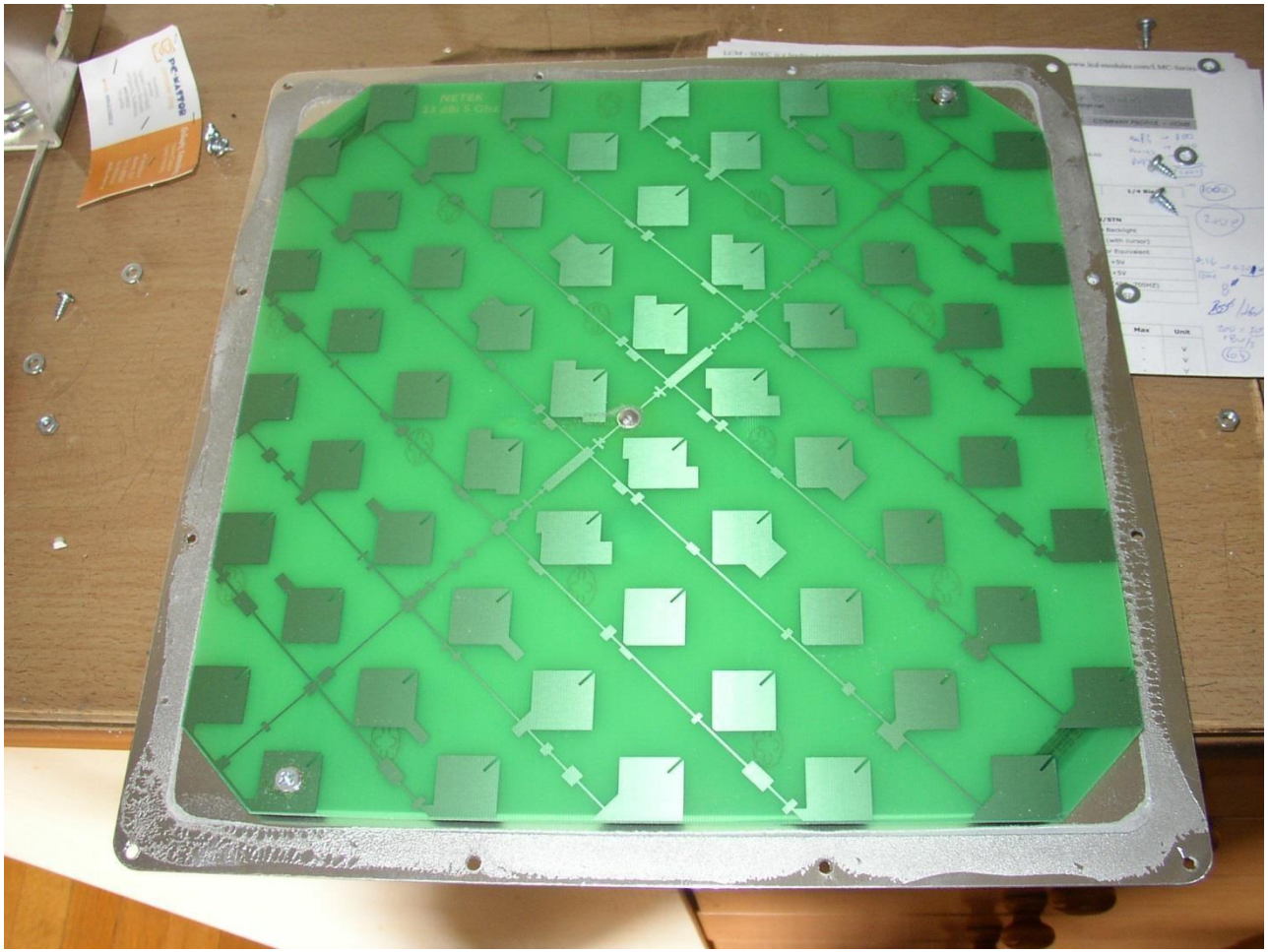
The airMAX 900 MHz YAGI is a high-gain array antenna designed to seamlessly integrate with the Rocket M900 radio (sold separately).It features incredible range performance (20+km) and breakthrough speed (90+Mbps real TCP/IP).

- Frequency Range: 902-928 MHz
- Dimensions: 66.5x11.6x11.6in (1690x295x295mm)
- Weight: 10.3lbs (4.65kg)

Our Price: $129.99

MSRP: $200.00 You Saved $70.01

Panel (or Patch) Antenna



- From digdice.com

Patch Antenna

Cisco Aironet Antenna Kit Patch Antenna

$30 online

Write a review

May 2000 - Wi-Fi - Indoor - Cisco - 9 dBi gain

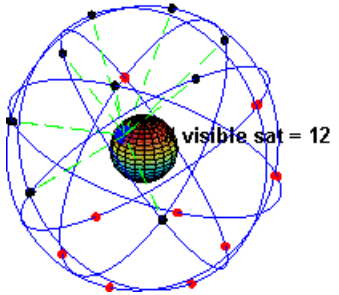
Cisco Systems, with proven reliability and robust product design, pr
professionals. Remote bridges connect hard-to-wire sites, noncontigu
settings, temporary networks, and ... more »

How-To: Build a WiFi biquad dish antenna

By Eliot Phillips *posted November 15th 2005 2:45PM*

Global Positioning System (GPS)

- Location using signals from a set of satellites
- Works with war-driving software to create a map of access points



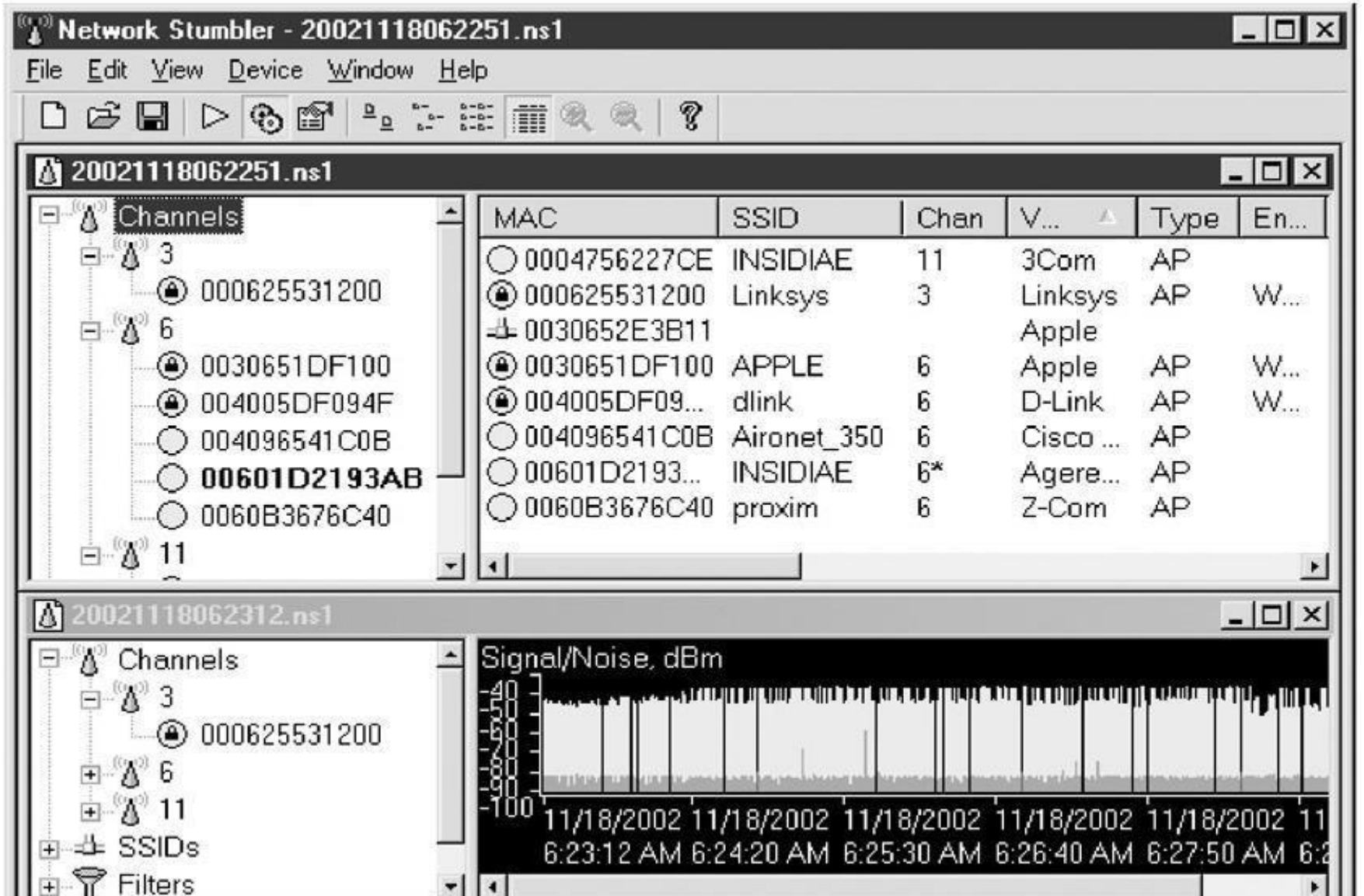
Discovery and Monitoring

- Discovery tools use 802.11 management frames
  - Probe requests/responses
  - Beacons
- Source and destination addresses of an 802.11 frame is always unencrypted
  - Tools can map associations between clients and APs

Finding Wireless Networks

- Active Discovery
  - Send out broadcast probe requests
  - Record responses
  - Misses APs that are configured to ignore them
  - NetStumbler does this
- Passive Discovery
  - Listen on every channel
  - Record every AP seen (their MAC)
  - Much better technique

NetStumbler Screen

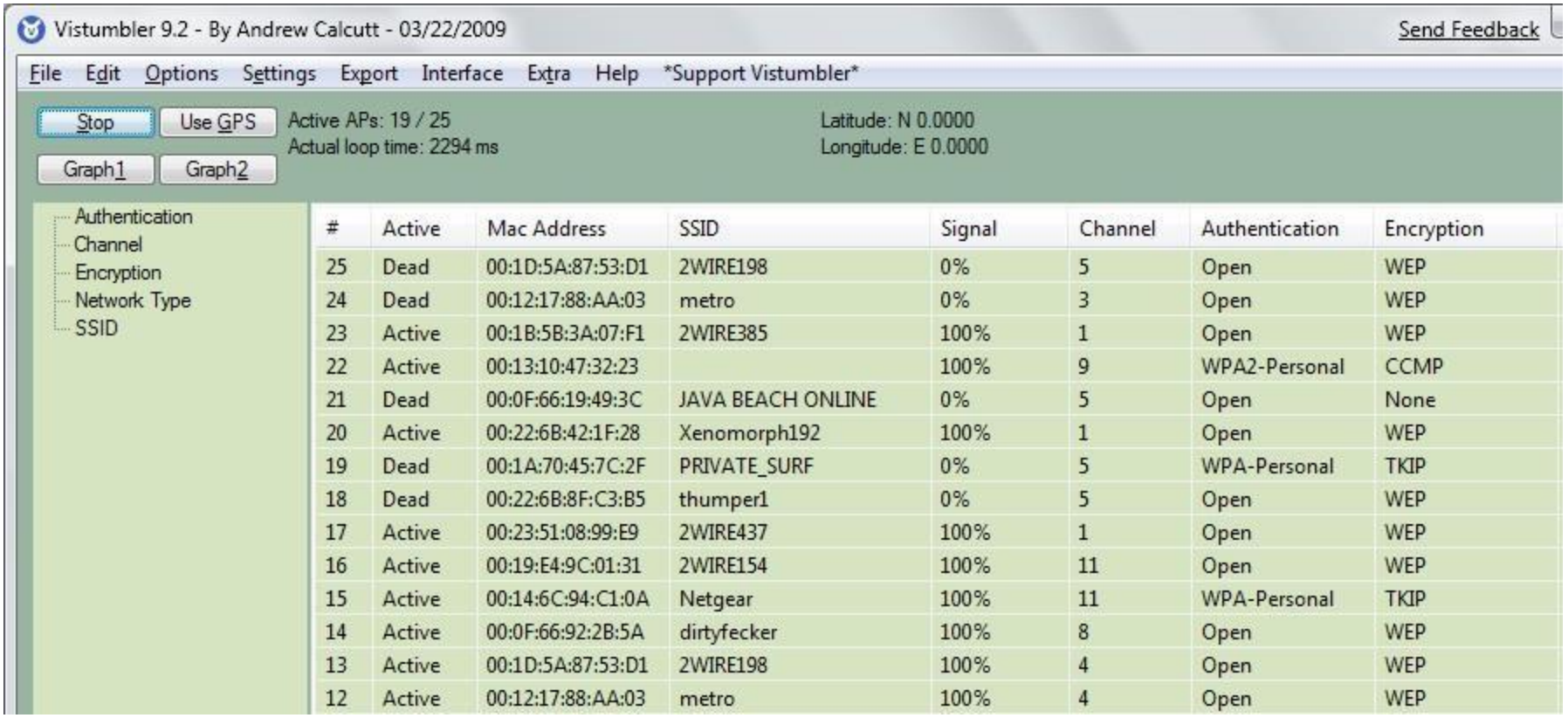


Wardriving

Wardriving

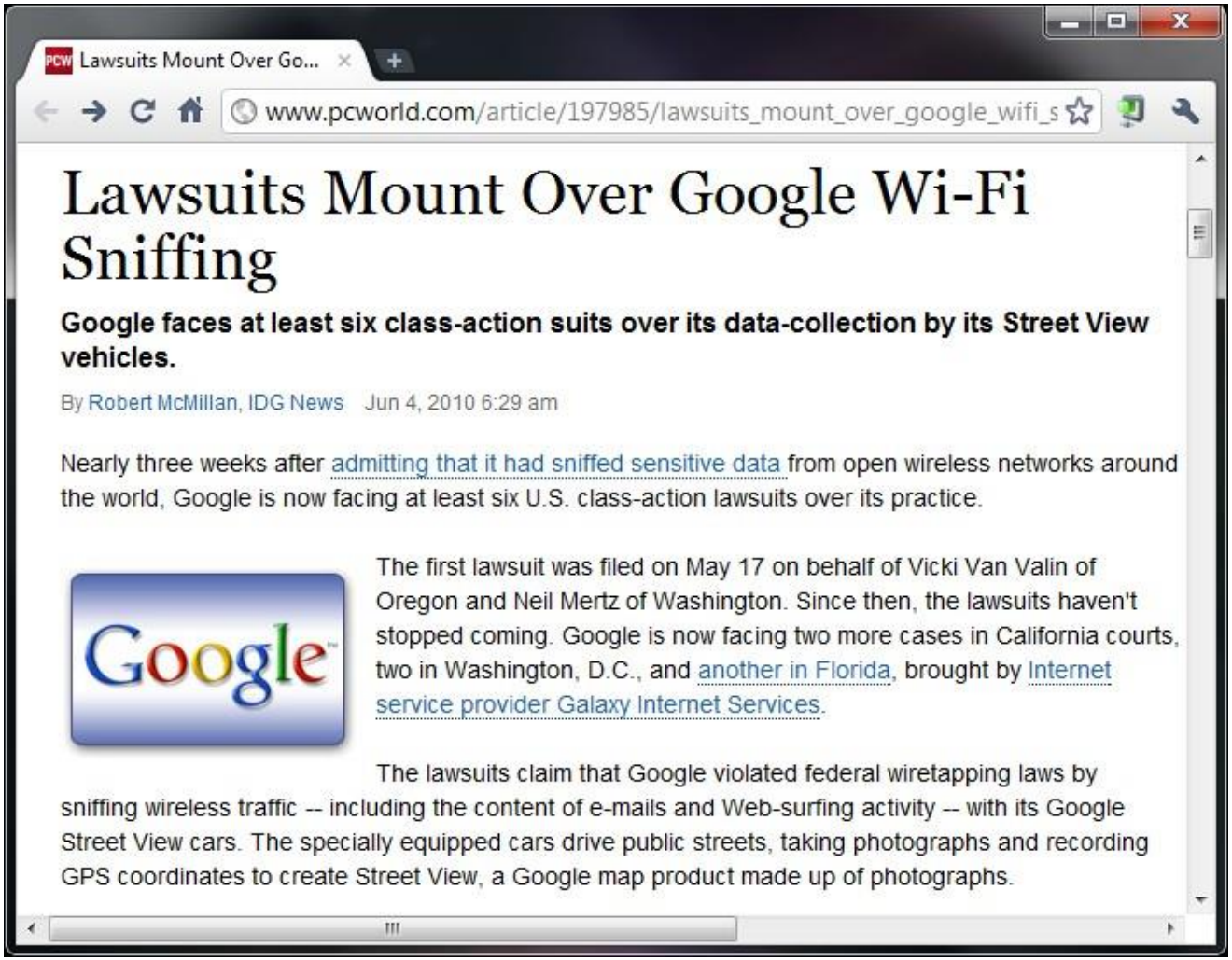
- Finding Wireless networks with a portable device
  - Image from overdrawn .net

Vistumbler



#	Active	Mac Address	SSID	Signal	Channel	Authentication	Encryption
25	Dead	00:1D:5A:87:53:D1	2WIRE198	0%	5	Open	WEP
24	Dead	00:12:17:88:AA:03	metro	0%	3	Open	WEP
23	Active	00:1B:5B:3A:07:F1	2WIRE385	100%	1	Open	WEP
22	Active	00:13:10:47:32:23		100%	9	WPA2-Personal	CCMP
21	Dead	00:0F:66:19:49:3C	JAVA BEACH ONLINE	0%	5	Open	None
20	Active	00:22:6B:42:1F:28	Xenomorph192	100%	1	Open	WEP
19	Dead	00:1A:70:45:7C:2F	PRIVATE_SURF	0%	5	WPA-Personal	TKIP
18	Dead	00:22:6B:8F:C3:B5	thumper1	0%	5	Open	WEP
17	Active	00:23:51:08:99:E9	2WIRE437	100%	1	Open	WEP
16	Active	00:19:E4:9C:01:31	2WIRE154	100%	11	Open	WEP
15	Active	00:14:6C:94:C1:0A	Netgear	100%	11	WPA-Personal	TKIP
14	Active	00:0F:66:92:2B:5A	dirtyfecker	100%	8	Open	WEP
13	Active	00:1D:5A:87:53:D1	2WIRE198	100%	4	Open	WEP
12	Active	00:12:17:88:AA:03	metro	100%	4	Open	WEP

Google Sniffing



Smartphone

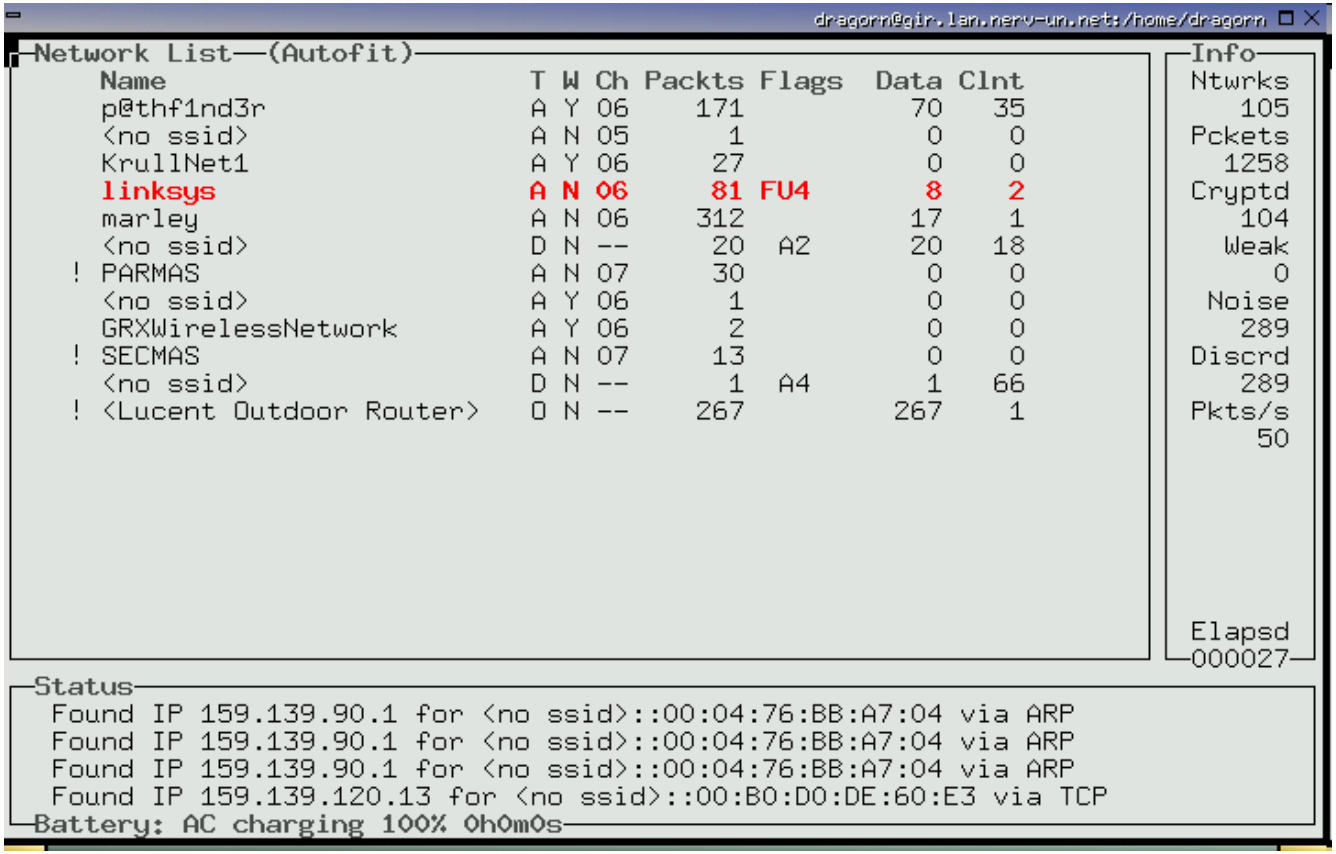
- The iPhone combines GPS, Wi-Fi, and cell tower location technology to locate you

- You can wardrive with the Android phone and Wifiscan

WiGLE

- Collects wardriving data from users
- Has over 16 million records
  - Link Ch 825

Kismet Screenshot

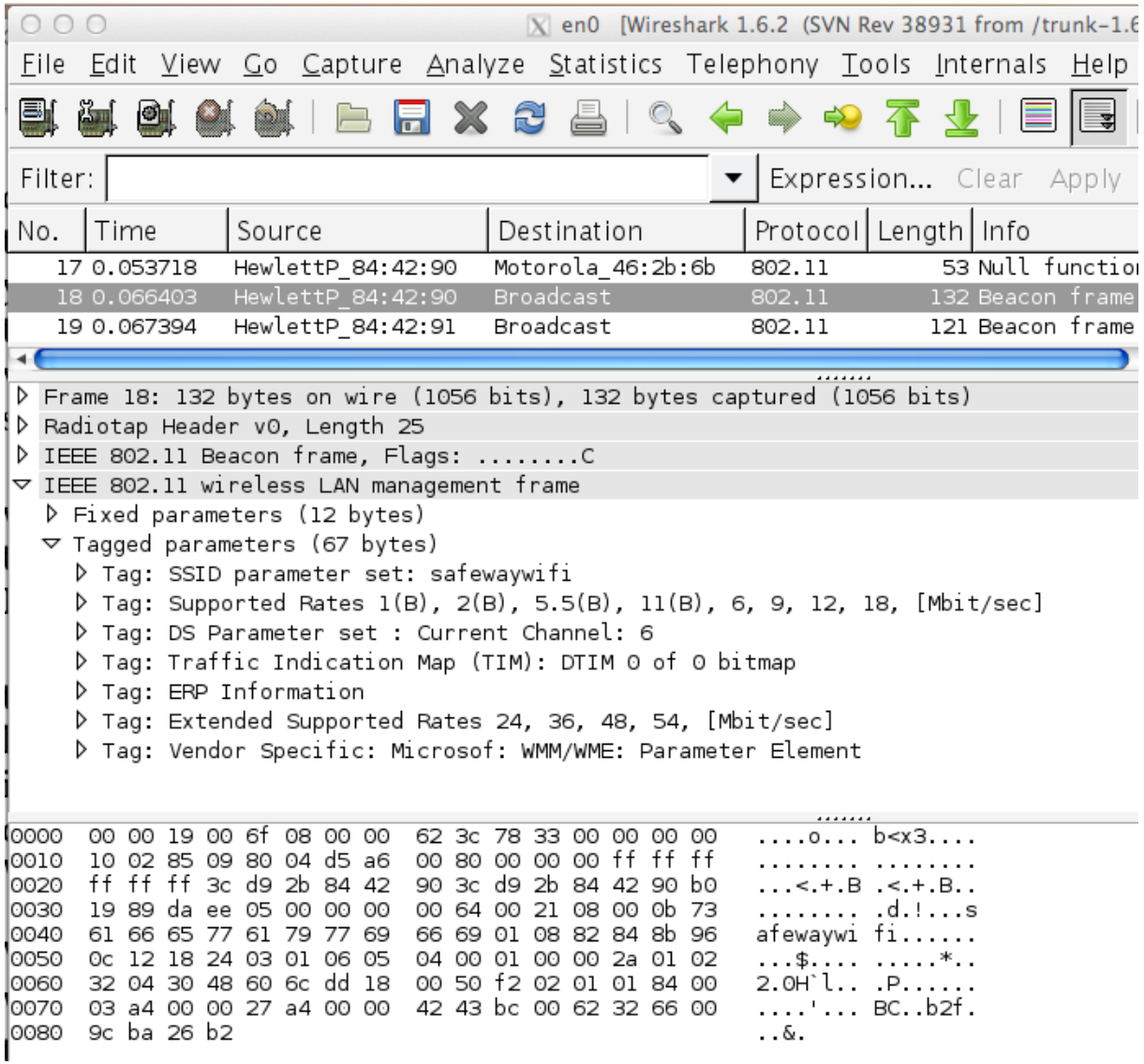


- Also airodump-ng: part of aircrack-ng, simpler than Kismet

Sniffing Wireless Traffic

- Easy if traffic is unencrypted
- Man-in-the-middle (MITM) attacks common and easy
- May violate wiretap laws
- If you can't get you card into "Monitor mode" you'll see higher level traffic but not 802.11 management frames
- Kismet saves sniffed traffic to a PCAP file

Wireshark: Wireless Sniffing on Mac



De-authentication DoS Attack

- 802.11 built-in mechanism: forced disconnect
  - Incorrect encryption key, overloading, etc.
  - Abused for DoS attacks
- Unauthenticated Management Frames
  - An attacker can spoof a de-authentication frame that looks like it came from the access point
  - airplay-ng: part of aircrack-ng
    - Deauth attack: 64 deauth to AP from client, 64 deauth to client from AP
    - Find SSID by observing client's probe requests as it reconnects

Identifying Wireless Network Defenses

SSID

- SSID can be found from any of these frames
  - **Beacons**
    - Sent continually by the access point (unless disabled)
  - **Probe Requests**
    - Sent by client systems wishing to connect
  - **Probe Responses**
    - Response to a Probe Request
  - **Association and Reassociation Requests**
    - Made by the client when joining or rejoining the network
- If SSID broadcasting is off, just send a deauthentication frame to force a reassociation

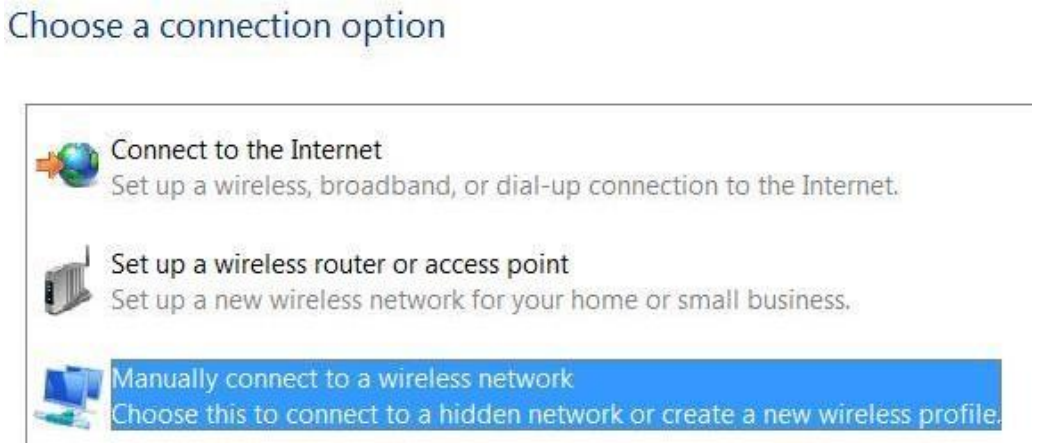
MAC Access Control

- CCSF used this technique for years
- Each MAC must be entered into the list of approved addresses
- High administrative effort, low security
- Attacker can just sniff MACs from clients and spoof them

Gaining Access
(Hacking 802.11)

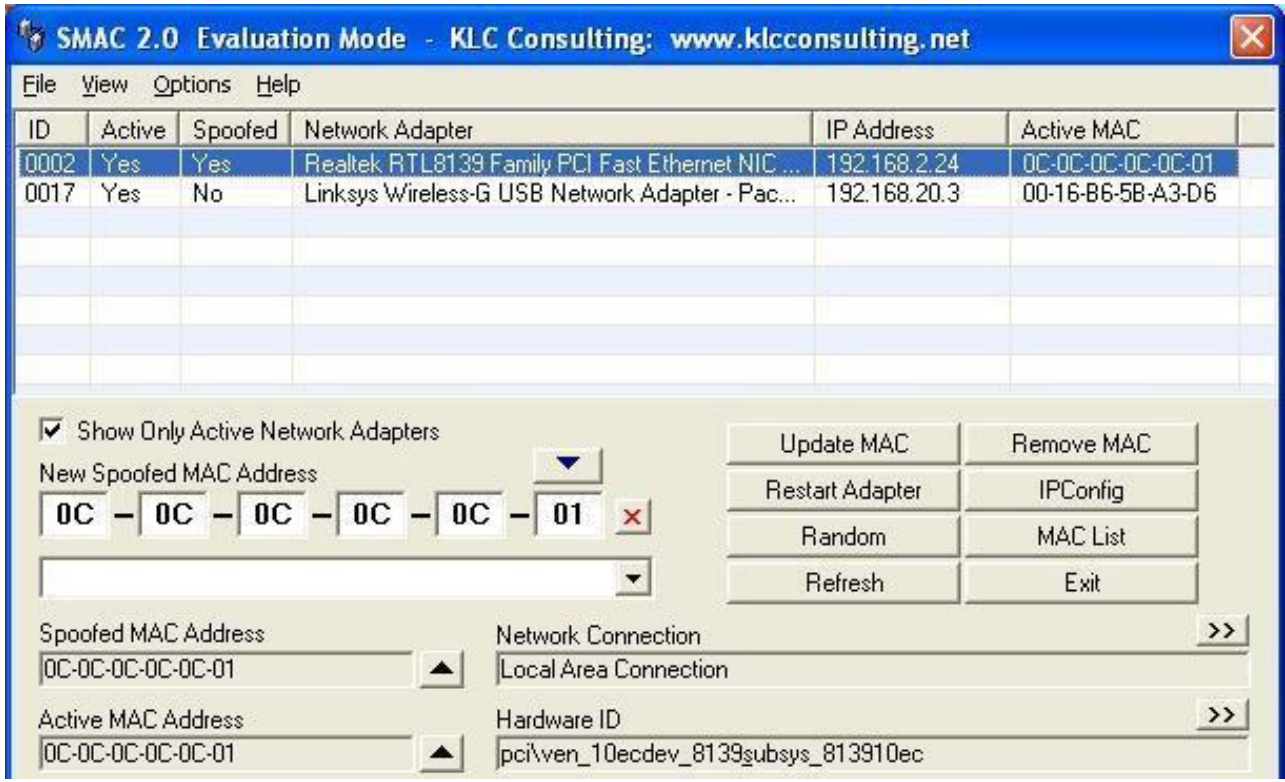
Specifying the SSID

- In Windows, just select it from the available wireless networks
  - In Vista, right-click the network icon in the taskbar tray and click "Connect to a Network"
  - If the SSID is hidden, click "Set up a connection or network" and then click "Manually connect to a wireless network"



Changing your MAC

- Bwmachak changes a NIC under Windows for Orinoco cards
- SMAC is easy



Device Manager

- Many Wi-Fi cards allow you to change the MAC in Windows' Device Manager

Attacks Against the WEP Algorithm

- Brute-force keyspace – takes weeks even for 40-bit keys
- Collect Initialization Vectors, which are sent in the clear, and correlate them with the first encrypted byte
  - This makes the brute-force process much faster

Tools that Exploit WEP Weaknesses

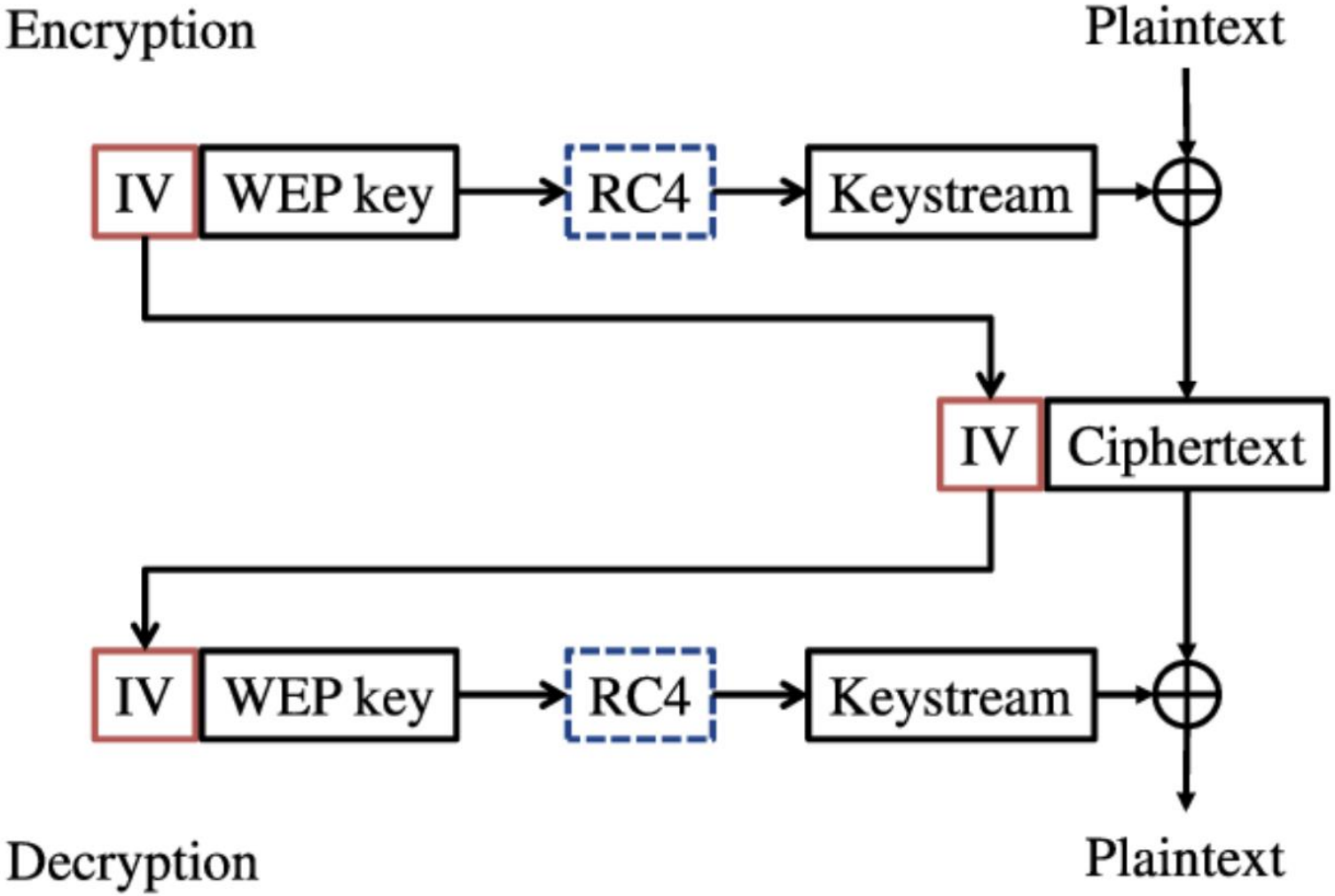
- AirSnort
- WLAN-Tools
- DWEPCrack
- WEPAttack
  - Cracks using the weak IV flaw
- Best countermeasure – use WPA

Encryption Attacks

- WPA vs. WEP
  - /w authentication vs. /wo authentication
  - /w key rotation vs. /wo key rotation
  - Crack again and again vs. crack once for all
- WEP
  - Keystream
    - Generated by WEP key and IV (Initiation Vector, pseudo-randomly generated for each frame and put into frame header)
    - TX: XOR plain text to get cipher text
    - RX: Use WEP key and IV from frame header to generate a keystream, XOR cipher text to get plain text

Encryption Attacks

WEP



Source: Watanabe, Morii - Proposal of WEP Operation with Strong IV and Its Implementation

Encryption Attacks

- WPA vs. WEP
  - /w authentication vs. /wo authentication
  - /w key rotation vs. /wo key rotation
  - Crack again and again vs. crack once for all
- WEP
  - Keystream
    - Generated by WEP key and IV (Initiation Vector, pseudo-randomly generated for each frame and put into frame header)
    - TX: XOR plain text to get cipher text
    - RX: Use WEP key and IV from frame header to generate a keystream, XOR cipher text to get plain text
  - Duplicate IVs in two frames → compare their cipher texts → guess the keystream → guess WEP key
  - ARP frames with little or no difference → more duplicate IVs → easier to guess the keystream and WEP key

Encryption Attacks
Passive Attack

- Capture enough data frames, parse IVs, deduce WEP key
  - 60,000 IVs to crack a 104-bit key
- airodump-ng: capture to a PCAP file
- aircrack-ng: analyze statistically on a PCAP file to get WEP key
  - Watch the rate at which IVs are collected to tell how much longer it will take to gather enough to crack the key
  - Stops with KEY FOUND

Encryption Attacks
ARP Replay with Fake Authentication

- Replay broadcast ARP requests
  - From a client to an AP
  - AP broadcasts with a new IV each time
  - The client replays ARP and generates new ARP
  - In 5 minutes, enough frames and IVs collected
- Spoof a valid client's MAC address
  - Fake authentication attack
    - Open authentication without sending actual data
- Steps
  - airodump-ng: capture to a PCAP file
  - aireplay-ng: run fake authentication attack
  - Open another window to launch ARP replay attack with aireplay-ng again
  - aircrack-ng: crack on the captured PCAP file
- WEP countermeasures: Don't use WEP ever.

WPA

- WPA - no major weaknesses until 2017
- However, if you use a weak Pre-Shared Key, it can be found with a dictionary attack
- But
  - PSK is hashed 4096 times, can be up to 63 characters long, and includes the SSID
- Tools: Airodump-ng, coWPAtty, rainbow tables

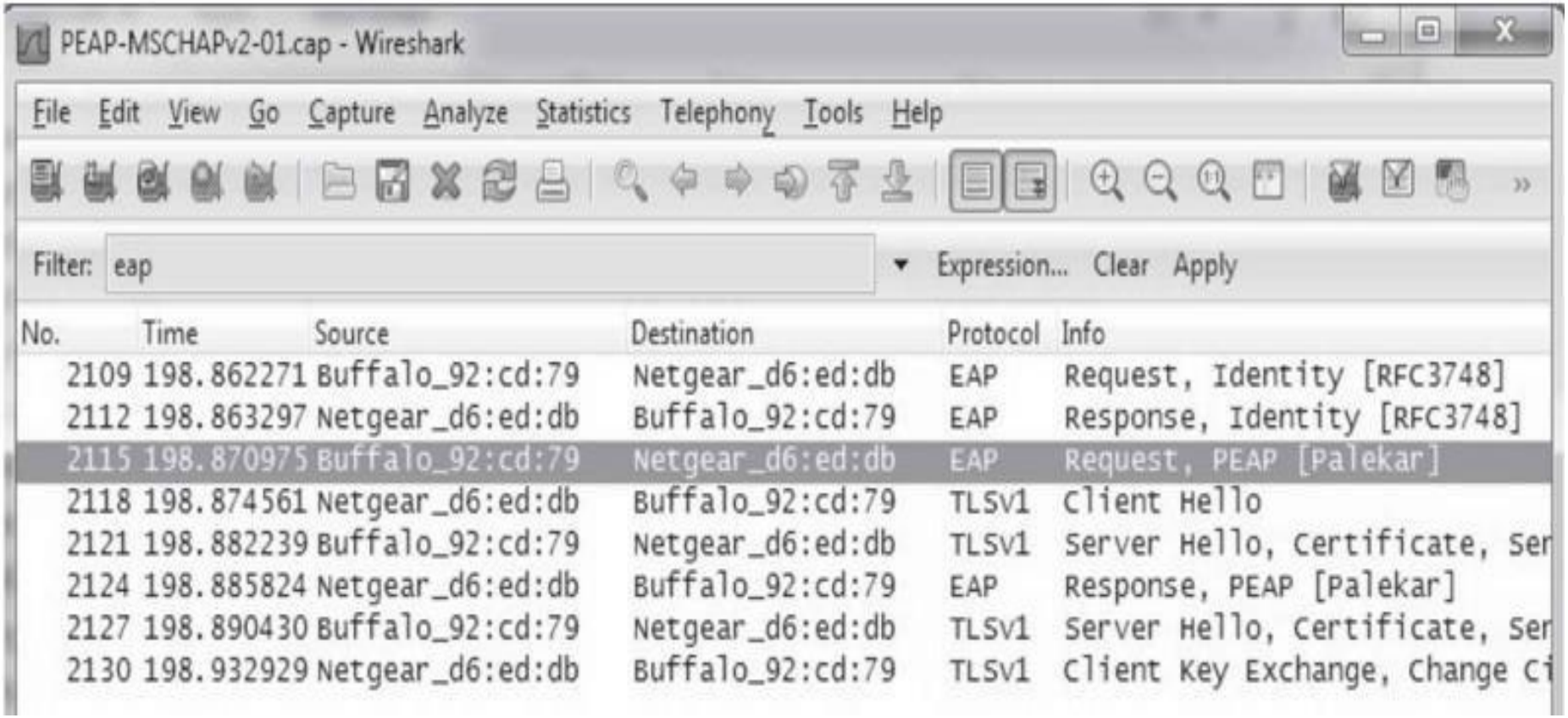
Authentication Attacks
WPA PSK

- About password brute forcing
- WPA PSK
  - PSK shared among all users of a wireless network
  - Four-way handshake between clients and APs: Using PSK and SSID to derive encryption keys
    - PSK, 8~63 characters, hashed 4096 times with SSID
    - Trillions of guesses
  - Capture four-way handshake to crack PSK offline
    - Wait or deauth to kick a client off (its driver will reconnect)
  - Brute forcing
    - aircrack-ng with dictionary and PCAP
    - coWPAtty: use SSID-specific rainbow tables (40GB)
      - Use top 1000 SSIDs from WiGLE.net
    - Pyrit: offload hashing to GPU with multiple cores
- WPA-PSK mitigating controls
  - Complex PSK and unique SSID
  - But could be disclosed by a single user

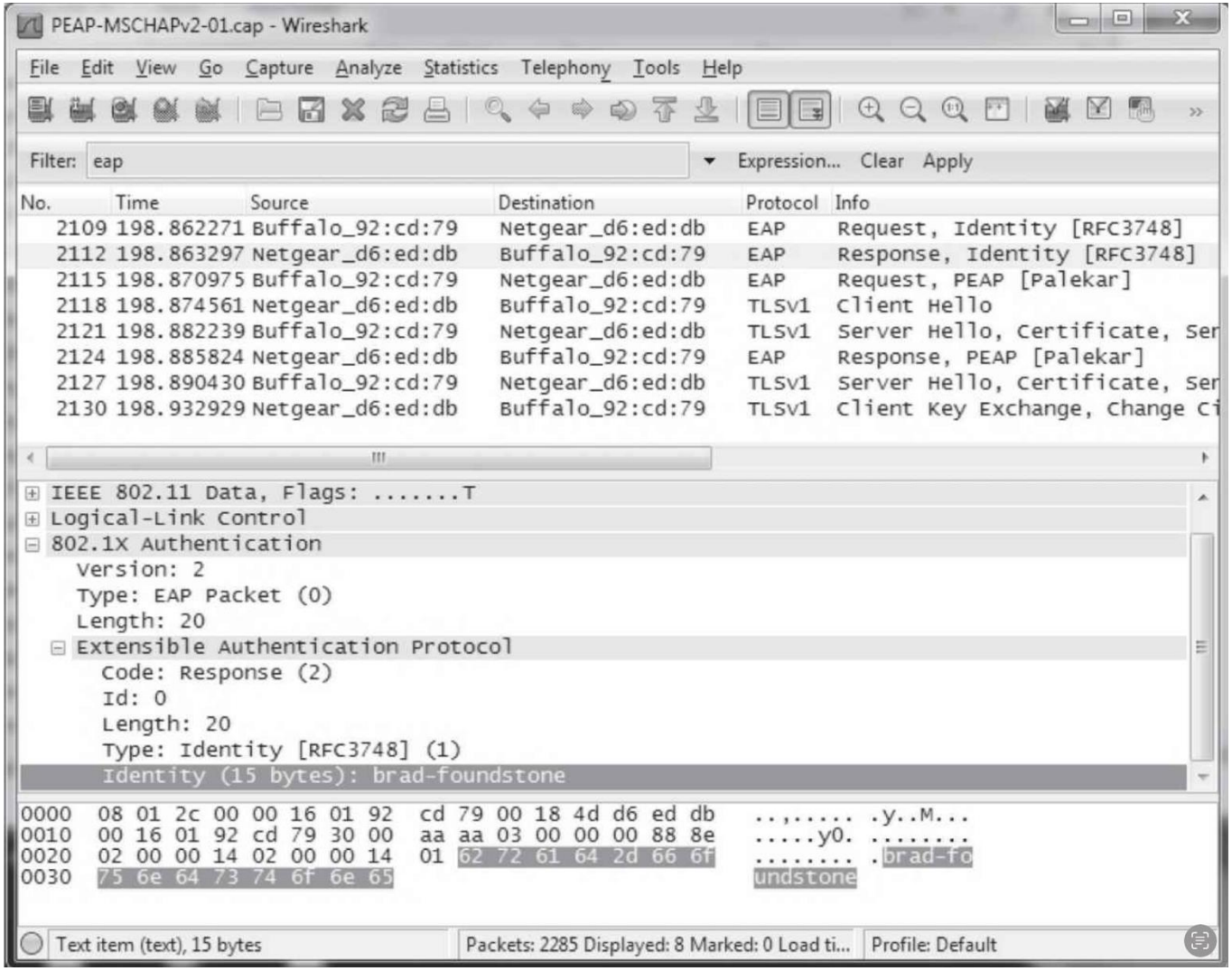
Attacking WPA Enterprise

- This means attacking **EAP** - **Extensible Authentication Protocol**
- Techniques depend on the specific EAP type used
  - LEAP
  - EAP-TTLS and PEAP

Detecting EAP type with Wireshark



Detecting username with Wireshark



Lightweight Extensible Authentication Protocol (LEAP)

What is LEAP?

- A proprietary protocol from Cisco Systems developed in 2000 to address the security weaknesses common in WEP
- LEAP is an 802.1X schema using a RADIUS server
- As of 2004, 46% of IT executives in the enterprise said that they used LEAP in their organizations

The Weakness of LEAP

- LEAP is fundamentally weak because it provides zero resistance to offline dictionary attacks
- It solely relies on MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) to protect the user credentials used for Wireless LAN authentication

MS-CHAPv2

- MS-CHAPv2 is notoriously weak because
  - It does not use a SALT in its NT hashes
  - Uses a weak 2 byte DES key
  - Sends usernames in clear text
- Because of this, offline dictionary and brute force attacks can be made much more efficient by a very large (4 gigabytes) database of likely passwords with pre-calculated hashes
  - Rainbow tables

Cisco's Defense

- LEAP is secure if the passwords are long and complex
  - 10 characters long with random upper case, lower case, numeric, and special characters
- The vast majority of passwords in most organizations do not meet these stringent requirements
  - Can be cracked in a few days or even a few minutes

Asleap

- Grabs and decrypts weak LEAP passwords from Cisco wireless access points and corresponding wireless cards
- Integrated with Air-Jack to knock authenticated wireless users off targeted wireless networks
  - When the user reauthenticates, their password will be sniffed and cracked with Asleap

Microsoft: Don't Use PPTP and MS-CHAP

22 August 2012, 09:51

« previous | next »

Microsoft says don't use PPTP and MS-CHAP

Microsoft is warning of a serious security issue in MS-CHAP v2, an authentication system that is mainly used in Microsoft's Point-to-Point Tunneling Protocol (PPTP) VPN technology. Three weeks ago at the Black Hat conference, encryption expert Moxie Marlinspike presented the CloudCracker web service, which can crack any PPTP connection within 24 hours for $200.

- Microsoft recommends PEAP, L2TP/IPsec, IPSec with IKEv2, or SSTP instead

EAP-TTLS and PEAP

Transport Layer Security (TLS) Tunnel

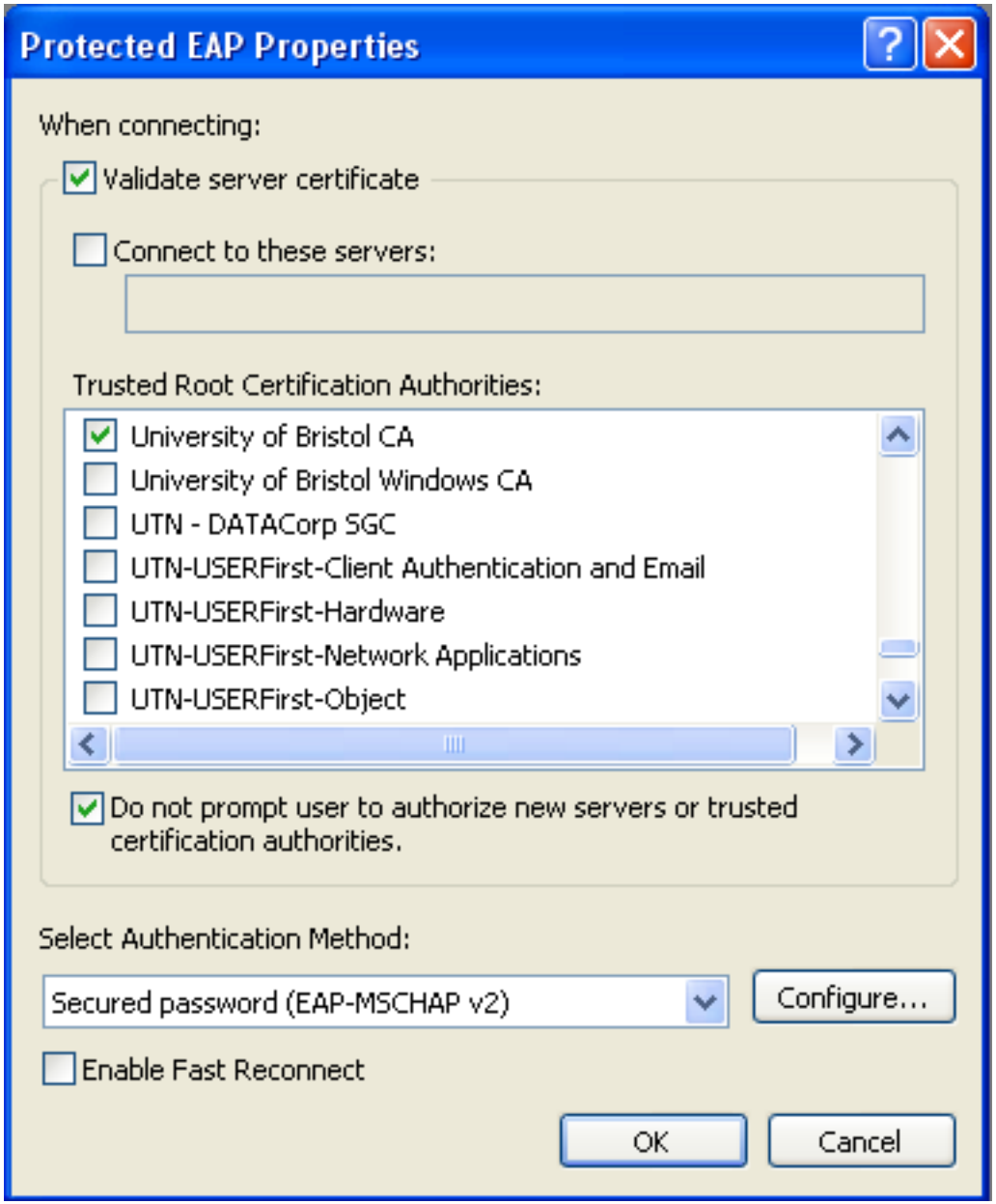
- EAP-TTLS and PEAP both use a TLS tunnel to protect a less secure *inner authenticated protocol*
- Inner authentication protocols
  - MS-CHAPv2
  - EAP-GTC (one-time passwords)
  - Cleartext

Attacking TLS

- No known way to defeat the encryption
- But AP impersonation can work
  - Trick target into connecting to MITM instead of server
  - Misconfigured clients won't validate the identity of the RADIUS server so it can be spoofed
  - FreeRADIUS-WPE: accepts any connections and outputs data to a log.

Protecting EAP-TTLS and PEAP

- Check the "Validate the Server Certificate" on all wireless clients



Authentication Attacks
WPA Enterprise

- Identifying 802.1x EAP (extensible authentication protocol) types
  - Capture EAP handshake
  - Wireshark shows EAP type
  - Unencrypted username in RADIUS server in EAP handshake
- LEAP (lightweight EAP)
  - Cisco solution /w clear text MSCHAPv2 challenge/response
  - asleep: offline brute-force attack with LEAP handshake and wordlist
  - Avoid using LEAP just like WEP
- EAP-TTLS and PEAP
  - A TLS (Transport Layer Security, successor of SSL) tunnel between an unauthenticated client and RADIUS server
    - AP relays and has no visibility
  - Less secure inner authentication protocol (often in clear text)
  - AP impersonation and man-in-the-middle attack
    - Act as a terminating end of the TLS tunnel, if the client is misconfigured not to check the identity of RADIUS server → access inner auth protocol
  - hostapd: Turn your card into an AP
  - asleep: offline brute-force on inner authentication protocol
  - Countermeasure: Check the box to validate server certificate on all clients

Summary

- WEP
  - Passive attack & ARP replay with fake authentication
  - Cracked in 5 min
  - Don’t use it!
- WPA-PSK
  - Could be brute-forced, though high complexity
  - One PSK fits all → put other users at risk
- WPA Enterprise
  - LEAP
    - Could be brute-forced, needs extremely complex passwords
    - Don’t use it!
  - EAP-TTLS and PEAP
    - Relatively secure with multilayered encryption
    - Subject to AP impersonation and man-in-the-middle attack
    - Always have clients check server certificate

Homework #5 Ch6-8

(format: problem, solution with explanation, screen dumps)

1. (30 points) Use all of WHOIS, Robtex, and PhishTank to trace back on a phishing email found in your mailbox. If you don't find one, create one email account and post the email address onto Web to solicit some. Show and discuss your findings.
2. (30 points) On Windows with some running processes connecting to the Internet, use FTK Imager to dump memory and then Volatility Framework to analyze the memory dump. Show processes with connections, and check whether they have DLLs.
3. (30 points) Retrieve Poison Ivy RAT from the Internet. Use a program tracing tool you are familiar with to trace this RAT. Show how you trace the RAT with your tracing tool and summarize what modules this RAT contains.
4. (20 points) Use Nmap, NTA Monitor, IKEProbe to identify whether a target VPN server supports Aggressive mode. Screen dump "useful" results and explain.
5. (30 points) Setup your own client and an AP, or find an existing AP, running no encryption. Use wireshark or airodump-ng to sniff and decode data frames. Show and discuss your findings.
6. (50 points) Setup your own client and an AP to run WEP. Use the aircrack-ng suite to crack the WEP key by running through the steps of frame capturing, fake authentication attack, ARP replay attack, and key cracking. Show and discuss the steps you run through.