

Wi-Fi Security

How to Break and Exploit

Hallvar Hellesest

Department of Informatics, UiB, Norway

Outline

- Introduction
- How to identify Wi-Fi networks
 - Analyzing Wi-Fi network traffic
 - Demonstration and results from *warbiking*
- Breaking the security of Wi-Fi networks
 - Description of some vulnerabilities
 - Demonstration of WEP key recovery
- Exploiting access to Wi-Fi networks
 - Identity concealment
 - Information gathering
- Summary and conclusion

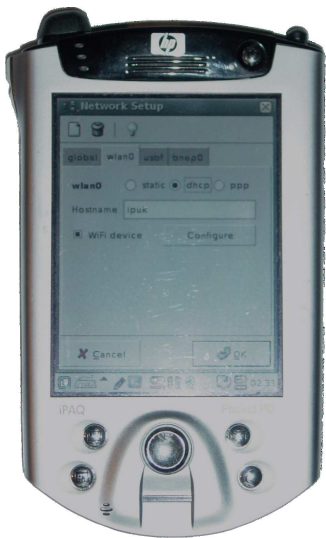
Introduction

Wireless-Fidelity (Wi-Fi):

- Technology to enable inexpensive wireless communication between consumer level computer devices
- Final standard IEEE 802.11 of 1999
- 802.11 includes security specification termed Wired Equivalent Privacy (WEP)
- WEP has a numerous amount of security flaws
- Wi-Fi Protected Access (WPA) replaces and improves upon WEP
- Possibility of WPA key recovery when installed in a common fashion.
- Widespread and vulnerable, leads to exploitation

How to Identify Wi-Fi Networks

Requires off-the-shelf hardware equipment, publicly available software tools and a mobile computer platform. Some modifications may be necessary to create an optimal setup when breaking and exploiting.

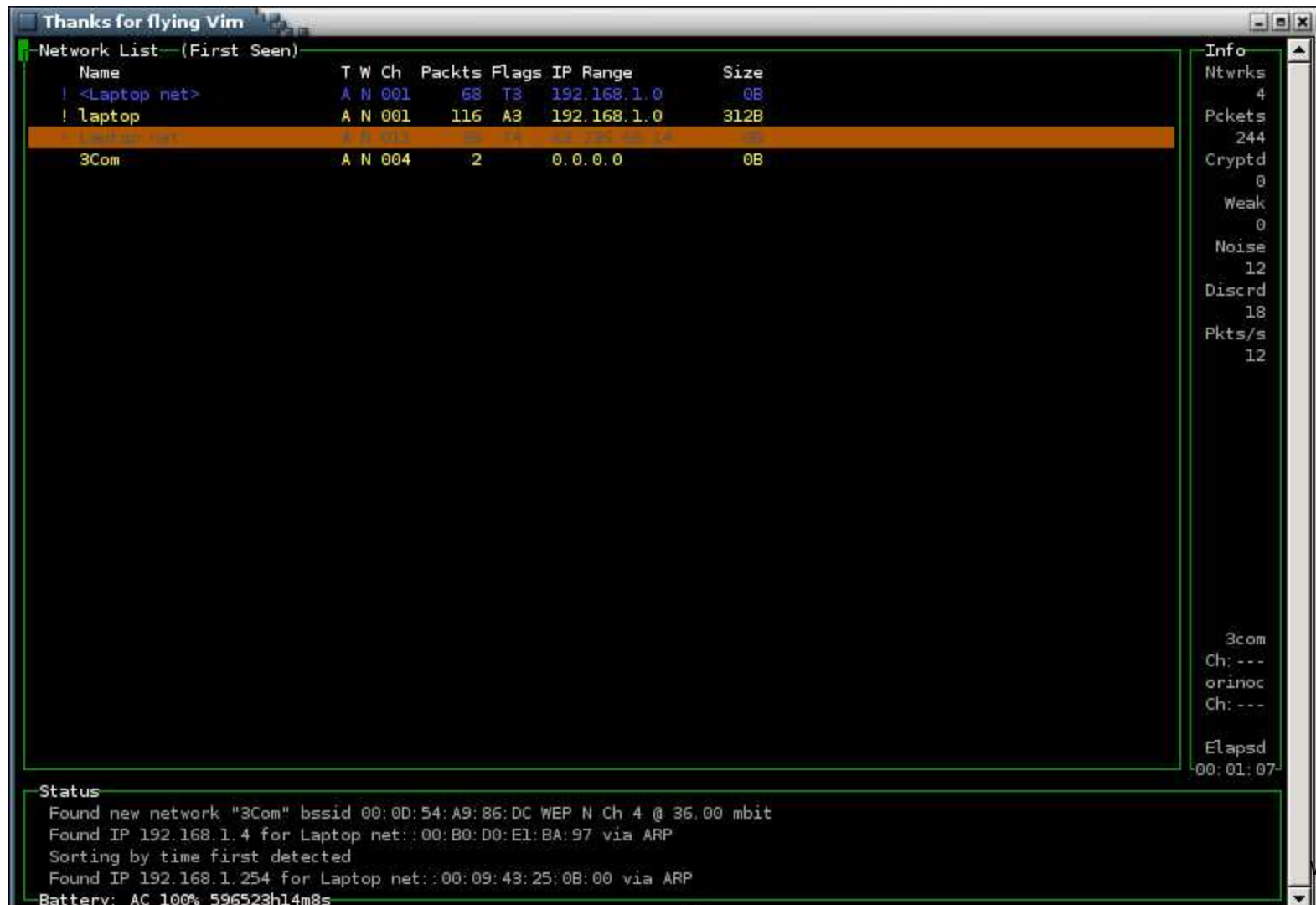


Analyzing Wi-Fi Network Traffic

- WEP or WPA enabled
- Ad-hoc/Infrastructure network
- SSID with interesting names
- MAC addresses
- Contents of data
- Network range
- Physical location of transmitters

Demonstration of Network Discovery

Kismet is a software tool to identify Wi-Fi networks and analyze its traffic. [Link to video of Kismet.](#)



The screenshot shows a terminal window titled "Thanks for flying Vim" displaying the Kismet network discovery interface. The main window is titled "Network List (First Seen)" and contains a table of discovered networks. The table has columns for Name, T, W, Ch, Packts, Flags, IP Range, and Size. The networks listed are: <Laptop net>, laptop, and 3Com. The "laptop" network is highlighted in orange. To the right of the table is an "Info" panel showing statistics for the selected network, including Ntwrks (4), Pckets (244), Cryptd (0), Weak (0), Noise (12), Discrd (18), and Pkts/s (12). Below the main window is a "Status" panel showing the following information: Found new network "3Com" bssid 00:0D:54:A9:86:DC WEP N Ch 4 @ 36.00 mbit, Found IP 192.168.1.4 for Laptop net::00:B0:D0:E1:BA:97 via ARP, Sorting by time first detected, Found IP 192.168.1.254 for Laptop net::00:09:43:25:0B:00 via ARP, and Battery: AC 100% 596523h14m8s.

Name	T	W	Ch	Packts	Flags	IP Range	Size
<Laptop net>	A	N	001	68	T3	192.168.1.0	0B
! laptop	A	N	001	116	A3	192.168.1.0	312B
3Com	A	N	004	2		0.0.0.0	0B

Info

Ntwrks 4
Pckets 244
Cryptd 0
Weak 0
Noise 12
Discrd 18
Pkts/s 12

3com
Ch: ---
orinoc
Ch: ---
Elapsd 00:01:07

Status

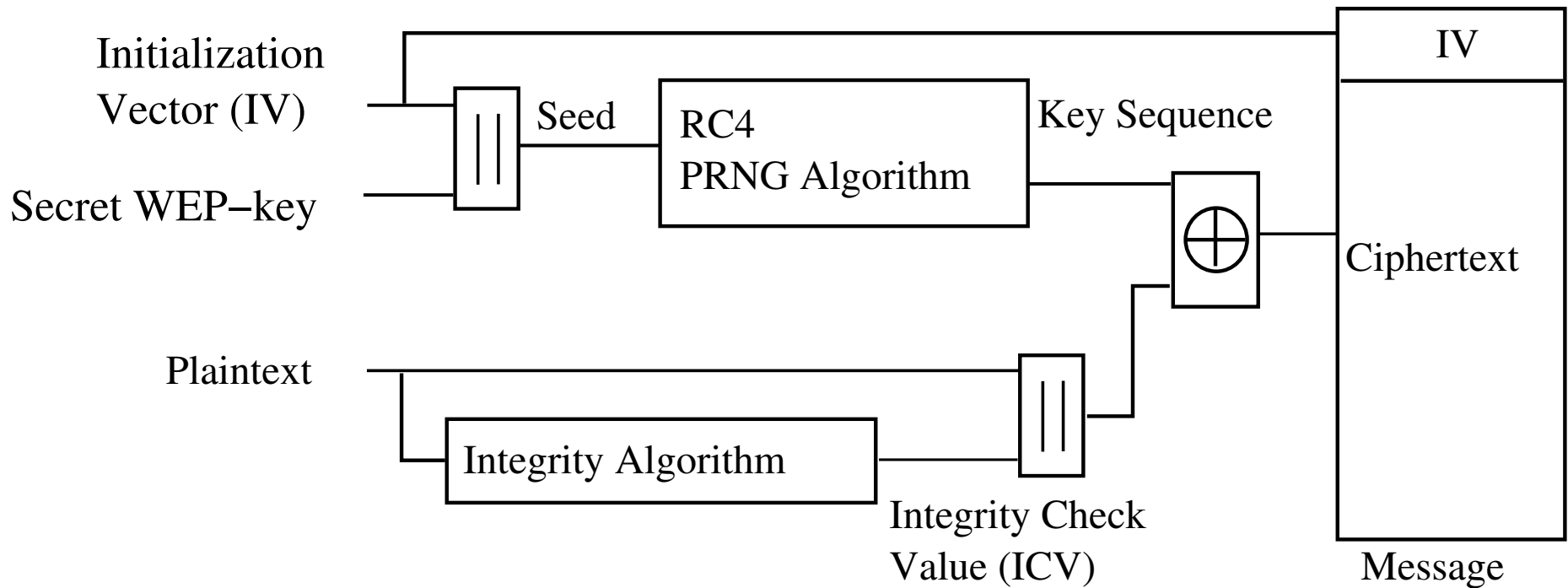
Found new network "3Com" bssid 00:0D:54:A9:86:DC WEP N Ch 4 @ 36.00 mbit
Found IP 192.168.1.4 for Laptop net::00:B0:D0:E1:BA:97 via ARP
Sorting by time first detected
Found IP 192.168.1.254 for Laptop net::00:09:43:25:0B:00 via ARP
Battery: AC 100% 596523h14m8s

Statistics from Warbiking

Performed February 6th 2005.

- 374 networks/access points discovered in 1 hour
- 67 % (251) do not use WEP or WPA

Breaking the Security of Wi-Fi Networks



Security services of WEP and WPA:

- Confidentiality
- Authentication
- Access control

Breaking Confidentiality of WEP

- Recover WEP key—RC4 key scheduling weakness.
- Recover a passphrase seeded WEP key.
- Double encryption.
- Inductive chosen plaintext attack.
- IV and key sequence database.
- Redirecting packets.
- Brute-force the WEP key.

RC4 Key Scheduling Weakness

- When using RC4, some bytes of some keys leak into the key sequence
- Using statistical analysis, the key can be recovered
- 300,000 to 2,000,000 key sequences and IVs can result in a recovered key
- Attack published in 2001 and improved in 2004

Inductive Chosen Plaintext

Can obtain an arbitrarily long key sequence.

1. Capture an encrypted packet which seems interesting.
2. Guess with high certainty the first n bytes of the data.
3. Calculate the ICV over the $n - 3$ bytes.
4. Concatenate the $n - 3$ bytes and the ICV then XOR it with the matching key sequence.
5. Append a brute-force guessed byte.
6. The packet is transmitted to the access point.
7. If the packet is valid, the last byte is the last byte of the ICV. The actual decrypted value of it is at this point unknown. However, since all bytes before the last byte is known, applying the CRC on the known data to construct the ICV will reveal the real value of the last byte—and thus the byte of the key sequence.
8. If the packet is invalid, go to step 5 and guess the value of the last byte to something else.

Inducing Network Traffic

- Recovering a key with the RC4 key scheduling weakness requires a lot of encrypted packet
- Some networks are low traffic, thus the collection process can take a long time, days, weeks or months
- An attacker can force access points or clients to transmit encrypted frames at a fast rate
- ARP requests can be retransmitted to have a valid client reply
- With a key sequence, arbitrary packets can be injected and cause a client to reply

In tests approximately 800 encrypted packets/second were induced. At this rate 1,000,000 packets are captured in 21 minutes.

Demonstration of Breaking WEP

A session where a WEP encrypted network was attacked and the key recovered after 40 minutes.

[Link to video of Aircrack.](#)

Breaking Confidentiality of WPA

- Recovering a passphrase seeded WPA key.

WPA provides protection against *data* packet injection and retransmission. Management frames are still vulnerable.

Recovering PMK of WPA-PSK

Dictionary attack against a WPA-enabled Wi-Fi network.

$PMK = PBKDF2(\textit{passphrase}, \textit{ssid}, \textit{ssidLength}, 4096, 256)$

To validate a guessed PMK, the initial WPA handshake is required.

1. Force a client to re-authenticate and perform the handshake
2. Capture an encrypted packet
3. Generate a PMK from a guessed passphrase
4. From guessed PMK and handshake, generate MIC key
5. Decrypt packet with the appropriate key and recalculate the MIC using the guessed MIC key
6. If there is a match on the captured MIC and the recalculated MIC, the guessed passphrase is very likely to be correct

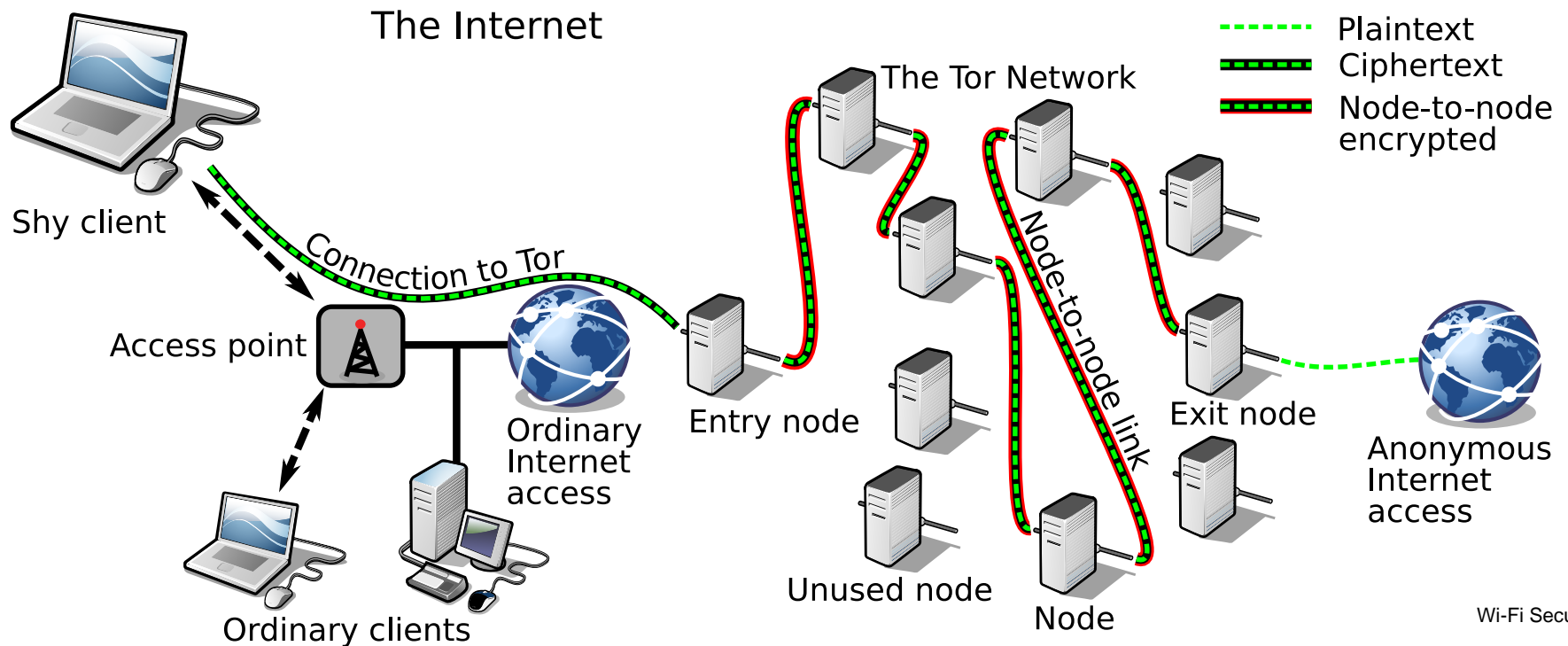
Exploiting Access to Wi-Fi Networks

- Identity concealment
 - Wi-Fi network users only see an encrypted stream of packets going to an anonymizing network
 - Good idea to change to a random MAC address
- Scanning and monitoring a Wi-Fi network

Identity Concealment

Network intruders can control the revelation of their identity.

- The contents of the packets are unknown to everyone except the exit node and final destination
- The destination of the packets are unknown to everyone except the exit node
- The origin of the packets are unknown to everyone except the entry node
- The nodes do not know the path of the circuit except their own source and destination



Possibilities with Tor

- Steal Internet access from your neighbor, and login to your personal e-mail account. The neighbor will not find out, by looking at the traffic, who is using his network.
- Operate as an international spy. Attacked government A, spying government U.
 - Spy must make sure A does not know he is contacting U.
 - Government must make sure the information from the spy really is from the spy
 - A, who captures information going into U and going out of their country, must not be able to discover that intelligence data is coming from country A and into U

Scanning and Monitoring

Direct access to communication and services on an internal network.

- Find computers on the network
- Find and access services on the computers
- Cleartext passwords
- Cleartext protocols, e.g. Internet browsing, e-mail, etc

Summary

Attack	Service	Requirements
RC4	Confidentiality, Authentication	300,000 WEP encrypted frames
WEP dictionary	Confidentiality, Authentication	Pass-phrase seeded key, 1 data frame
Chosen plaintext	Confidentiality	WEP enabled. Allow 10 byte data size
Redirect	Confidentiality	WEP enabled
Double encryption	Confidentiality	Internet connection
One way auth	Authentication	Shared-key authentication
Spoofing	Authentication	1 active and authenticated client
Rogue access point	Authentication	1 client
Packet injection	Access control	Known IV/key sequence
Profiling	Access control	Known IV/key sequence
MAC filter	Access control	MAC filter enabled
Captive Portal	Access control	MAC filter access control
WPA-PSK dictionary	Confidentiality, Authentication	Pass-phrase seeded key, handshake

Summary, continued

- WEP provides false sense of security
- Sometimes WPA too
- Vulnerable Wi-Fi networks are valuable to many

Conclusion

- Don't trust a Wi-Fi network
- Never use WEP
- Use WPA with a random and strong passphrase where possible
- Don't rely on Wi-Fi for anything mission critical
- Buy Wi-Fi equipment with 802.11i *and* use it