

## Lecture 14: More Wireless Hacking – Cracking Wired Equivalent Privacy (WEP)

### Legal Concerns

Defeating security to enter a network without permission is clearly illegal

- Even if the security is weak

Sniffing unencrypted wireless traffic may also be illegal

- It could be regarded as an illegal wiretap
- The situation is unclear, and varies from state to state
- In California, privacy concerns tend to outweigh other considerations
- See links 114v, 114w

### Equipment

Wireless Network Interface Cards (NICs) and Drivers

#### The Goal

All wireless NICs can connect to an Access Point

But hacking requires more than that, because we need to do

- *Sniffing* – collecting traffic addressed to other devices
- *Injection* – transmitting forged packets which will appear to be from other devices

#### Windows v. Linux

The best wireless hacking software is written in Linux

- The Windows tools are inferior, and don't support packet injection

But all the wireless NICs are designed for Windows

- And the drivers are written for Windows
- Linux drivers are hard to find and confusing to install

#### Wireless NIC Modes

There are four modes a NIC can use

- Master mode
- Managed mode
- Ad-hoc mode
- Monitor mode

See link 1\_14j

#### Master Mode

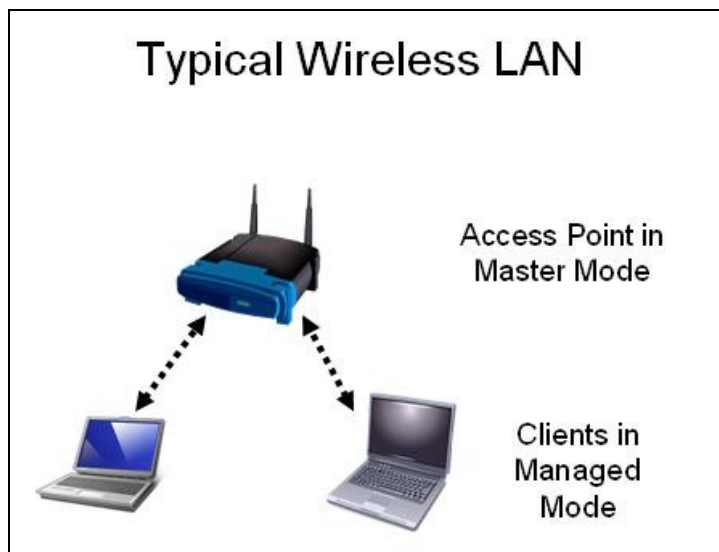
- Also called AP or Infrastructure mode
- Looks like an access point
- Creates a network with
  - A name (SSID)
  - A channel

#### Managed Mode

- Also called Client mode
- The usual mode for a Wi-Fi laptop
- Joins a network created by a master
- Automatically changes channel to match the master
- Presents credentials, and if accepted, becomes *associated* with the master

#### Ad-hoc Mode

- Peer-to-peer network
- No master or Access Point
- Nodes must agree on a channel and SSID



# Lecture 14: More Wireless Hacking – Cracking Wired Equivalent Privacy (WEP)

## Monitor Mode

- Does not associate with Access Point
- Listens to traffic
- Like a wired NIC in Promiscuous Mode

## Wi-Fi NICs

To connect to a Wi-Fi network, you need a Network Interface Card (NIC)

## PCMCIA

The most common type is the PCMCIA card

- Designed for laptop computers

## USB

- Can be used on a laptop or desktop PC

## PCI

- Installs inside a desktop PC



PCMCIA



## Choosing a NIC

For penetration testing (hacking), consider these factors:

- Chipset
- Output power
- Receiving sensitivity
- External antenna connectors
- Support for 802.11i and improved WEP versions

## Wi-Fi NIC Manufacturers

Each wireless card has two manufacturers

- The card itself is made by a company like  
Netgear  
Ubiquiti  
Linksys  
D-Link  
many, many others
- But the chipset (control circuitry) is made by a different company

## Chipsets

To find out what chipset your card uses, you must search on the Web

- Card manufacturer's don't want you to know

Major chipsets:

- Prism
- Cisco Aironet
- Hermes/Orinoco
- Atheros
- There are others



PCI



# Lecture 14: More Wireless Hacking – Cracking Wired Equivalent Privacy (WEP)

## Prism Chipset

Prism chipset is a favorite among hackers

- Completely open -- specifications available
- Has more Linux drivers than any other chipset

See link l\_14d

Prism chipset is the best choice for penetration testing

HostAP Linux Drivers are highly recommended, supporting:

- NIC acting as an Access Point
- Use of the iwconfig command to configure the NIC

See link l\_14h

## Cisco Aironet Chipset

Cisco proprietary – not open

Based on Prism, with more features

- Regulated power output
- Hardware-based channel-hopping

Very sensitive – good for wardriving

- Cannot use HostAP drivers
- Not useful for man-in-the-middle or other complex attacks

## Hermes Chipset

Lucent proprietary – not open

Lucent published some source code for WaveLAN/ORiNOCO cards

Useful for all penetration testing, but require

- Shmoo driver patches (link l\_14l) to use monitor mode

## Atheros Chipset

The most common chipset in 802.11a devices

- Best Atheros drivers are MadWIFI (link l\_14m)
- Some cards work better than others
- Monitor mode is available, at least for some cards

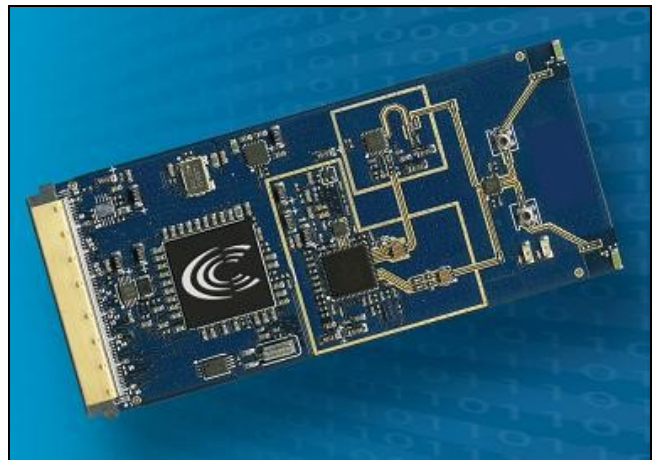
## Other Cards

If all else fails, you could use Windows drivers with a wrapper to make them work in Linux

- DriverLoader (link l\_14n)
- NdisWrapper (link l\_14o)

But all you'll get is basic functions, not monitor mode or packet injection

- Not much use for hacking



### PRISM GT Features and Benefits

- 802.11g Wi-Fi Certified™ up to 54 Mbps/2.4 GHz
- Backward compatible to all 802.11b products
- Most comprehensive security solution – Wi-Fi Protected Access™, Cisco compatible extensions (CCX), transport layer security (TLS), tunneled transport layer security (TTLS), message digest 5 (MD5), lightweight extensible authentication protocol (LEAP), and advanced encryption system (AES) with hardware acceleration

## Cracking WEP: Tools and Principles

### A Simple WEP Crack

The Access Point and Client are using WEP encryption

The hacker device just listens



## Lecture 14: More Wireless Hacking – Cracking Wired Equivalent Privacy (WEP)

### Listening is Slow

You need to capture 50,000 to 200,000 "interesting" packets to crack a 64-bit WEP key

- The "interesting" packets are the ones containing Initialization Vectors (IVs)
- Only about 1/4 of the packets contain IVs
- So you need 200,000 to 800,000 packets

It can take hours or days to capture that many packets

### Packet Injection

A second hacker machine injects packets to create more "interesting packet"

### Injection is MUCH Faster

With packet injection, the listener can collect 200 IVs per second

5 – 10 minutes is usually enough to crack a 64-bit key

Cracking a 128-bit key takes an hour or so

- Link 1\_14r

### AP & Client Requirements

#### Access Point

- Any AP that supports WEP should be fine (they all do)

#### Client

- Any computer with any wireless card will do
- Could use Windows or Linux

### Listener Requirements

NIC must support Monitor Mode

Could use Windows or Linux

- But you can't use NDISwrapper

#### Software

- Airodump (part of the Aircrack Suite) for Windows or Linux (see Link 1\_14q)
- BackTrack is a live Linux CD with Aircrack on it (and many other hacking tools)

Link 1\_14n

### Injector Requirements

NIC must support injection

Must use Linux

#### Software

- void11 and aireplay

Link 1\_14q

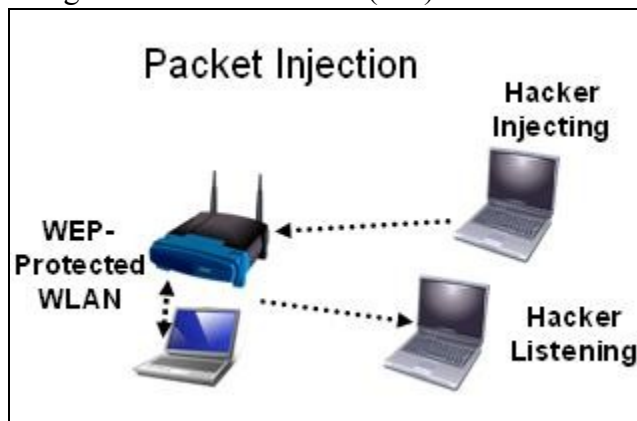
### Sources

[http://www.aircrack-ng.org/doku.php?id=compatible\\_cards](http://www.aircrack-ng.org/doku.php?id=compatible_cards) (link 1\_14a)

<http://www.wi-foo.com/> (link 1\_14c)

[http://www.vias.org/wirelessnetw/wndw\\_05\\_04.html](http://www.vias.org/wirelessnetw/wndw_05_04.html) (link 1\_14j)

<http://smallnetbuilder.com/content/view/24244/98/> (link 1\_14p)



Last modified 5-11-09