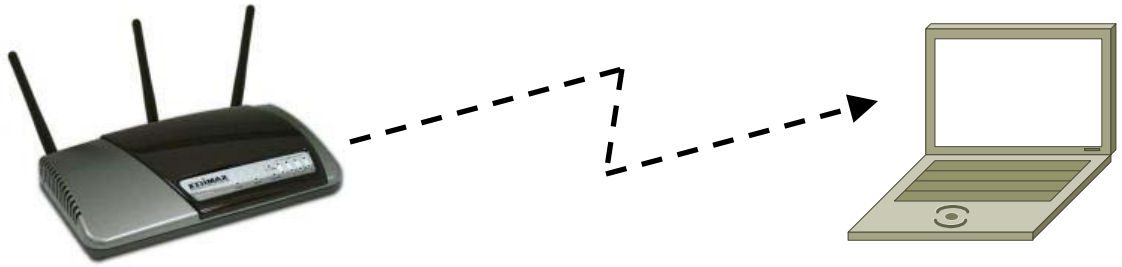
Wireless LAN Security I: WEP Overview and Tools



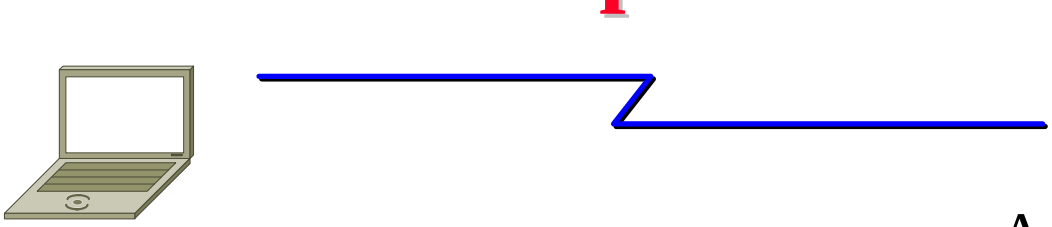
Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-09/

- Wi-Fi Operation
- Wired Equivalent Privacy (WEP)
- Problems with WEP
- Attack tools

Wi-Fi Operation



- Access Points (APs) periodically broadcast a beacon with SSID (service set ID) and security level
- Subscriber stations listen to these beacons, measure signal strength and determine which AP to join
- Subscribers can also send a "Probe" to find AP's in the neighborhood
- AP authenticates the subscriber station using shared keys
- Subscriber stations and AP exchange encrypted packets
- Subscriber station send a "Disassociate" message and log off

MAC Address Filtering

- Access Point contains MAC addresses of user NICs (Network Interface Cards)
- Prevents from casual guests logging into the wireless network
- Problem:
  - Easy to find good MAC addresses by sniffing and then address spoofing

Wired Equivalent Privacy (WEP)

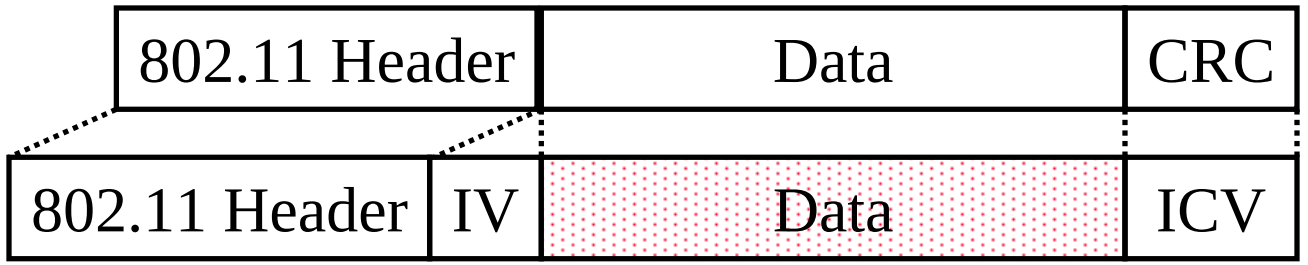
- WEP ⇒ Privacy similar to a wired network
  ⇒ Intellectual property not exposed to casual browser
  ⇒ Not protect from hacker
- First encryption standard for wireless. Defined in 802.11b
- Provides authentication and encryption
- Shared Key Authentication
  ⇒ Single key is shared by all users and access points
- Two modes of authentication: Open system and Shared Key
- Shared Key: Challenge-response verifies client has the key
- Manual key distribution
- If an adapter or AP is lost, all devices must be re-keyed

WEP Keys

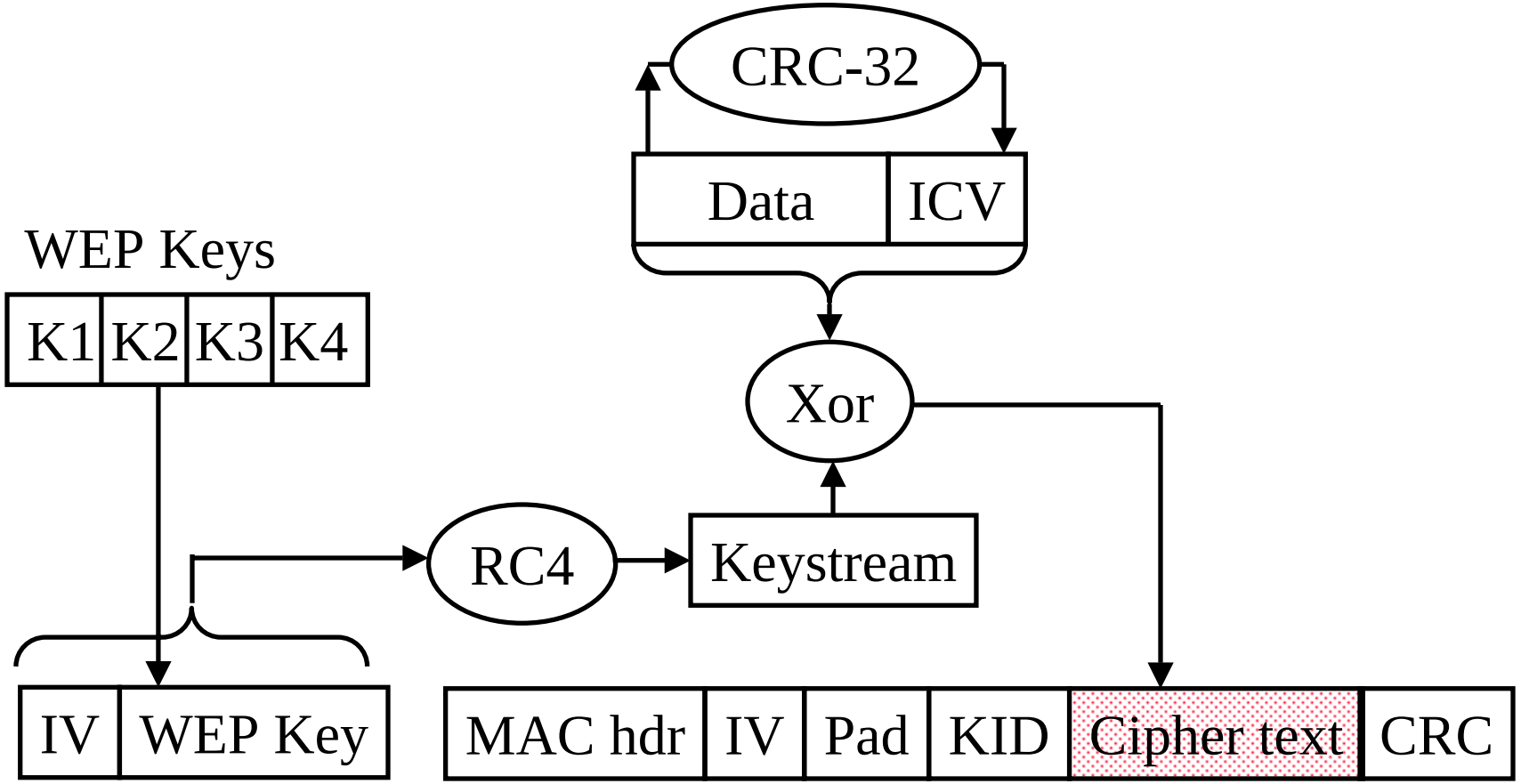
- **Default Key**: Also known as shared key, group key, multicast key, broadcast key. 40-bit or 104 bit. Static.
- **Key mapping key**: Also known as individual key, per-station key, unique key. Access points need to keep a table of keys. Not generally implemented.
- To allow smooth change over, two default keys are required (old and new).
- WEP allows 4 default keys. Keys are numbered 0..3.
  $\Rightarrow$ Can use different keys in two directions.
- Base key is combined with a 24-bit initialization vector (IV)
  $\Rightarrow$ Different key for each packet
- WEP does not specify how to select IV.
  Many vendors generate random IV.

WEP Details

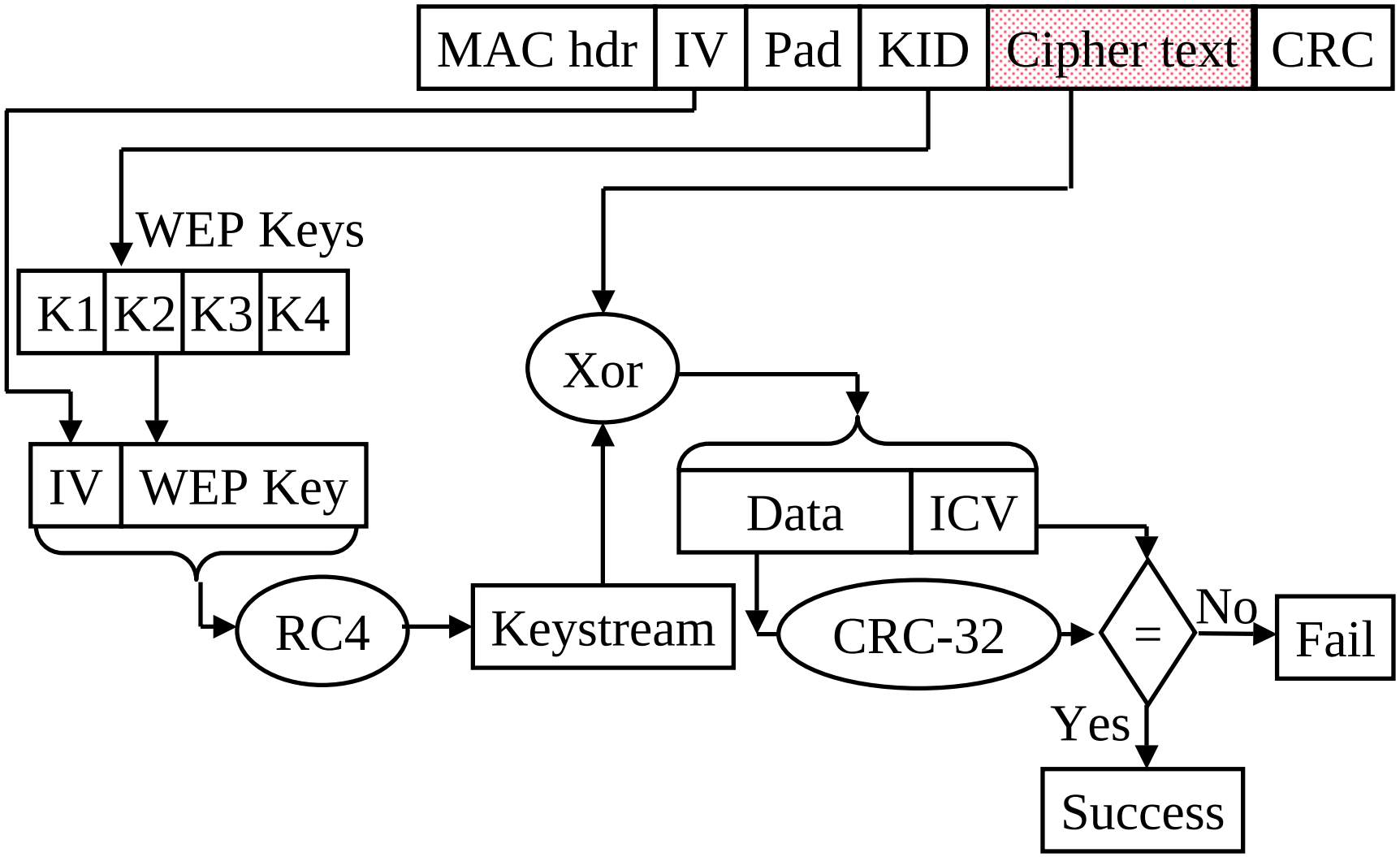
- Each device has 4 static WEP keys
- 2-bit key ID sent w Initialization Vector (IV) in clear in each packet
- Per-Packet encryption key =24-bit IV + one of pre-shared key
- Encryption Algorithm: RC4
  - Standard: 24 + 40 = 64-bit RC4 Key
  - Enhanced: 24 + 104 = 128 bit RC4 key
- WEP allows IV to be reused
- CRC-32 = Integrity Check Value (ICV)
- Data and ICV are encrypted under per-packet encryption key



WEP Encapsulation

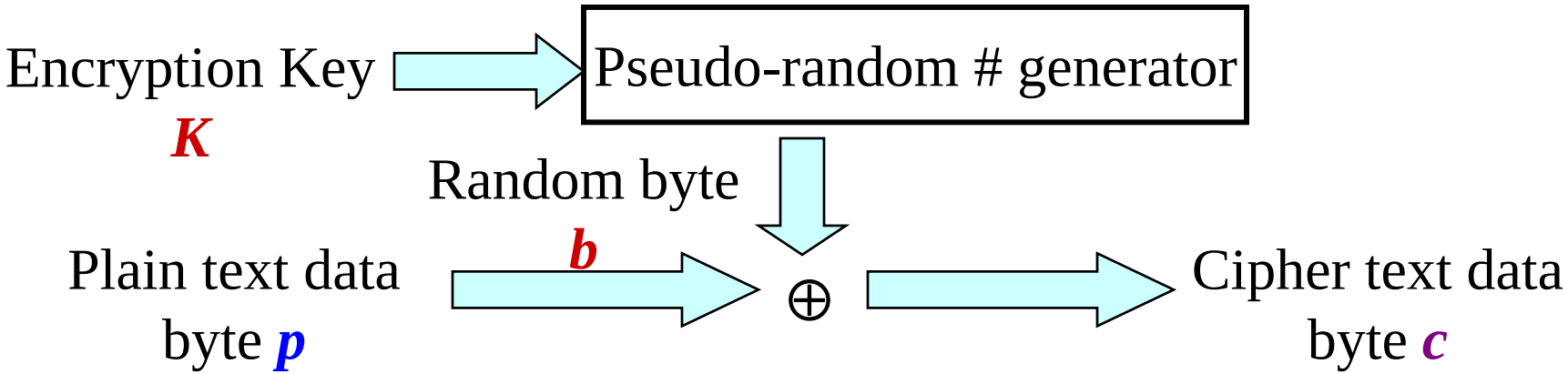


WEP Decapsulation



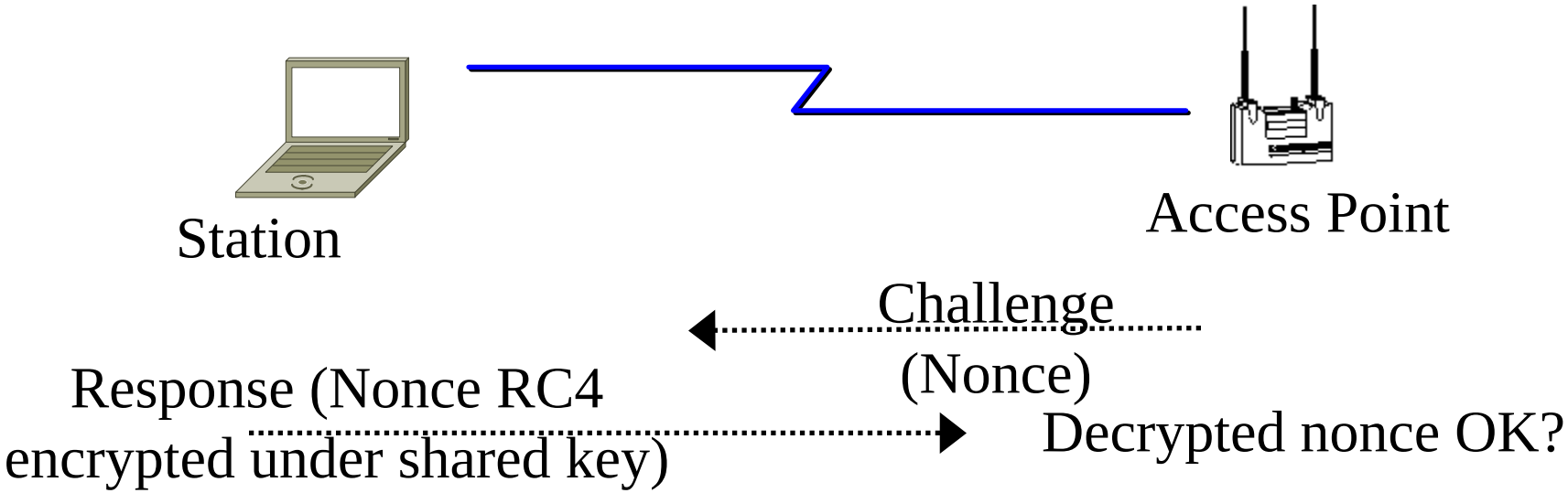
Ron's Cipher 4 (RC4)

- Developed by Ron Rivest in 1987. Trade secret. Leaked 1994.
- Stream Cipher
  - A pseudo-random stream is generated using a given key and xor'ed with the input
- Pseudo-random stream is called **One-Time pad**
- Key can be 1 to 256 octet
- See the C code in the textbook [KPS].



WEP Authentication

- Authentication is a via Challenge response using RC4 with the shared secret key.

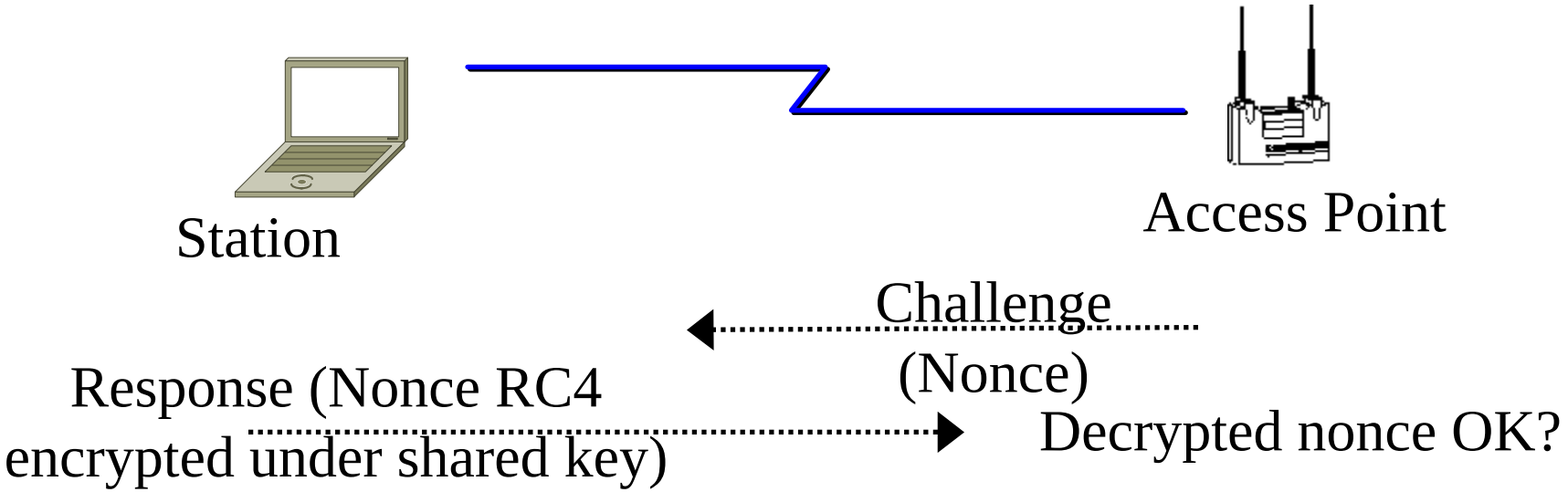


WEP Review

- Four 40-bit or 104-bit Keys are manually programmed in each subscriber station and AP
- A 24-bit IV and WEP key is used to form a 64b or 128b RC4 key
- A keystream is generated using the RC4 key
- A 32-bit CRC is added as "Integrity check value" (ICV) to the packet
- Plain text and keystream is xor'ed. A 32-bit CRC is added in clear.

Problems with WEP Authentication

- Record one challenge/response
- Both plain text and encrypted text are available to attacker
- XOR the two to get the keystream
- Use that keystream and IV to encrypt any subsequent challenges



Problem with Stream Cipher

- Consider two packets with the same IV $\Rightarrow$ Same keystream **b**
- **c**1 = **p**1 $\oplus$ **b**; **c**2 = **p**2 $\oplus$ **b** $\Rightarrow$ **c**1 $\oplus$ **c**2=**p**1 $\oplus$ **p**2
- Two packets w same IV $\Rightarrow$ XOR = Difference in plain text
- 50% chance of using the same IV in 4823 packets.
- Recovered ICV matches $\Rightarrow$ Plain text is correct
- Possible to recover all 2^{24} keystreams in a few hours

Problems with WEP ICV

- CRC is used as ICV
- CRC: Message polynomial is shifted and divided by CRC polynomial, the remainder is sent as CRC

$$\boldsymbol{p} = p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 x^0$$

- Remainder(**p**+**q**, c)
  = Remainder(**p**, c) + Remainder(**q**, c)
- ICV is linear: ICV(**p**+**q**) = ICV(**p**) + ICV(**q**)
- **Conclusion**: XOR any CRC-32 valid plain text to encrypted packet. The modified packet will pass the ICV after decryption.

More WEP Problems

- No centralized key management
  Manual key distribution ⇒ Difficult to change keys
- Single set of Keys shared by all ⇒ Frequent changes necessary
- No mutual authentication
- No user management (no use of RADIUS)
- IV value is too short. Not protected from reuse.
- Weak integrity check.
- Directly uses master key
- No protection against replay

Attack Tools

1. Tools to find wireless networks
2. Tools to monitor traffic
3. Tools to analyze traffic

Wardriving

- Driving by in a car to find open Wi-Fi networks
- Based on "War Dialing" to dial all numbers to find modem pools
- A commonly used tools is netsumbler, http://netstumbler.com/
- Also, **Warstrolling** and **Warflying**
- **Warchalking**: Signposting open acce on sidewalk or wall

Wardriving Tools

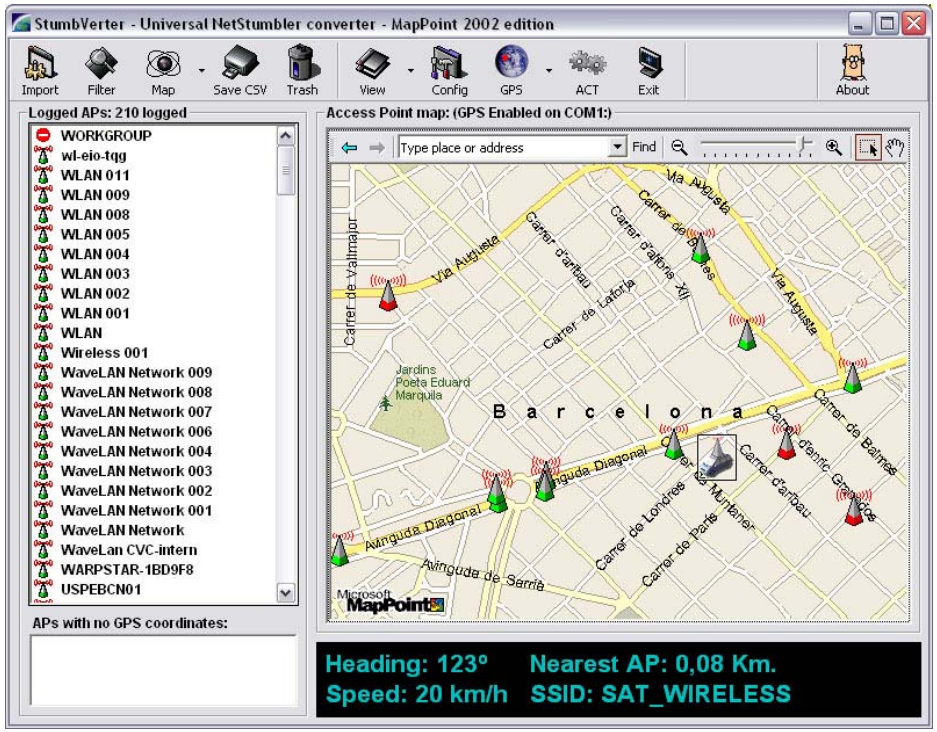
- See http://www.wardriving.com/code.php for a list of 40 wardriving tools

Sample

- Network stumbler, http://netstumbler.com
- Kismet, http://kismetwireless.net
- Mac Stumbler, http://www.macupdate.com/info.php/id/8035 for Macs
- KisMAC, http://en.wikipedia.org/wiki/KisMAC
- BSD Airtools: A set of free BSD tools for FreeBSD
  - dstumbler for wardriving - w GPS interface, http://www.bawug.org/howto/reviews/dstumbler.html
  - Bootable CD from www.warbsd.com

Network Stumbler

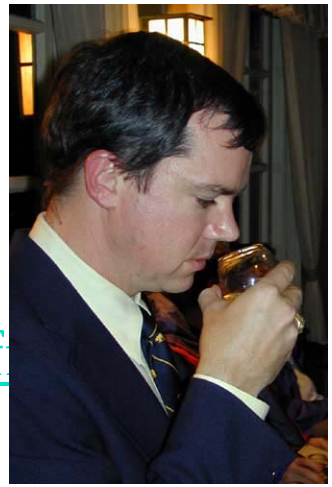
- Windows based
- Records SSIDs and can interface with GPS
- Ministumbler runs on PDAs and pocket PCs



Kismet

- http://kismetwireless.net
- Linux-base wardriving tool
- Reads out names of networks as they are discovered (eye-free feature for drivers)
- Can dump printable strings (may include passwords)
- List of networks in a CSV file
- Dump of all packets
- Dump of packets with weak IV
  $\Rightarrow$ for WEP key finding

Wireless Sniffing Tools



Public Domain:

- See list at http://wiki.personaltelco.net/WirelessSniff
- Airsnort (Linux / BSD?), http://airsnort.shmoo.com
- Airosniff (FreeBSD), http://www.freewebs.com/blacknet/download.html
- APsniff (Windows), http://www.monolith81.de/apsniff.html
- Aerosol (Windows), http://www.monolith81.de/mirrors/index.php?path=aerosol/
- Mognet (Java/Linux), http://www.monolith81.de/mognet.html
- Kismet (Linux), http://www.kismetwireless.net/
- Wellenreiter, http://sourceforge.net/projects/wellenreiter/

Wireless Sniffing Tools (Cont)

- wlandump (Linux-WLAN), http://www.linux-wlan.com/download.shtml
- WLAN Expert (Windows), http://www.vector.kharkov.ua/download/WLAN/wlanexpert.zip - More of a site survey tool

Commercial:

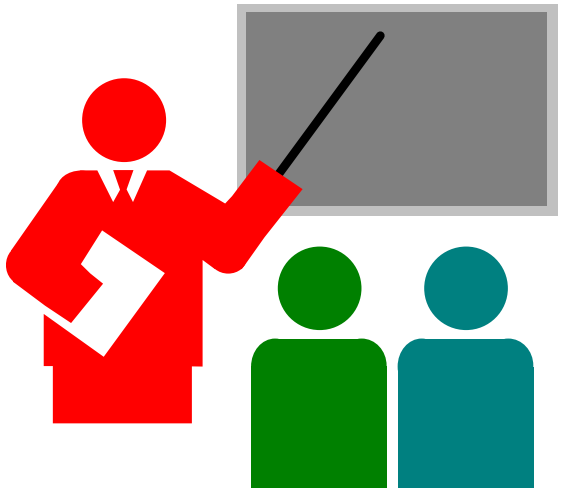
- Airopeek, http://download.cnet.com/AiroPeek/3000-2651_4-14808.html
- AP Scanner (Mac), http://ap-scanner.mac.findmysoft.com/
- Grasshopper, http://download.rhino3d.com/download_rel.asp?rel=427 - handheld wireless receiver
- Wireless Snif, www.ufasoft.com/sniffer/

More tools at http://www.wi-foo.com/index-3.html

Packet Analyzers

- Tcpdump, http://www.tcpdump.org/ , command-line network analyzer for UNIX
- windump, http://www.winpcap.org/windump/ , Windows version of tcpdump
- dSniff, http://www.monkey.org/~dugsong/dsniff/ , captures passwords
- omnipeek, http://www.wildpackets.com/ , packet analysis platform with plugin API
- snoop, http://en.wikipedia.org/wiki/Snoop_%28software%29 , command-line packet sniffer for Solaris
- Wireshark (aka Ethereal) (Linux or FreeBSD), http://www.wireshark.org
- Ngrep, http://ngrep.sourceforge.net/ -string matching in network traffic

Summary



- WEP uses RC4 stream cipher with a fixed set of keys
  $\Rightarrow$ Plain text is xor'ed with a keystream
- Authentication challenge is sent in clear
  $\Rightarrow$ getting keystream is trivial
- CRC is used for integrity $\Rightarrow$ Easy to modify
- Plenty of tools to find WiFi APs, monitor and analyze traffic
- Process of finding open APs is called Wardriving

Acronyms

- AP Access Point
- API Application Programming Interface
- BSD Berkeley System Distribution
- CD Compact Disk
- CRC Cyclic Redundancy Check
- CSV Comma Separated Values
- ICV Integrity Check Value
- ID Identification
- IV Initialization Vector
- MAC Media Access Control
- RADIUS Remote Authentication of Dial-In Users Service
- RC4 Ron's Code #4

Acronyms (Cont)

- SSID Service Set Identifier
- UNIX Named as a pun on MULTICS operating system
- WEP Wired Equivalant Privacy
- WLAN Wireless Local Area Networks
- WPA Wireless Protected Access
- XOR Exclusive-Or

Reading Assignment

Read

- Jesse Walker, "Unsafe at any Key Size. An Analysis of the WEP Encapsulation," Oct 2000, http://www.dis.org/wl/pdf/unsafew.pdf
- Abdel-Karim R. Al Tamimi , "Security in Wireless Data Networks : A Survey Paper," http://www.cse.wustl.edu/~jain/cse574-06/ftp/wireless_security/index.html
- Michale Roche, "Wireless Hacking Tools", http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html

References

The following books are on 2-hour reserve at the WUSTL Olin Library:

- J. Edney and W.A. Arbaugh, “Real 802.11 Security: Wi-Fi Protected Access and 802.11i,” Addison-Wesley, 2004, 481 pp., ISBN:0321156209
- Krishna Shankar, et al, "Cisco Wireless LAN Security," Cisco Press, 2005, 420 pp, ISBN:1587051540
- See also, 802.11 Security links, http://www.wardrive.net/security/links