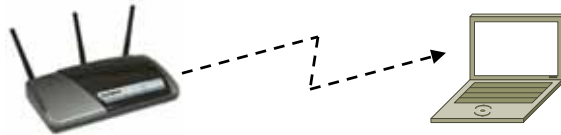


Wireless LAN Security I: WEP Overview and Tools



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/cse571-07/>

Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-1



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

Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-2

Wi-Fi Operation



Station



Access Point

- ❑ Access Points periodically broadcast a beacon with SSID 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
- ❑ 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)

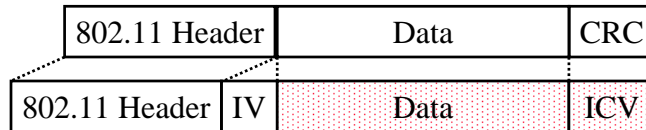
- ❑ WEP ⇒ Privacy similar to a wired network
 - ⇒ Intellectual property not exposed to casual browser
 - ⇒ Not protect from hacker
- ❑ First encryption standard for wireless. Defined in 802.11b
- ❑ Provides authentication and encryption
- ❑ Shared Key Authentication
 - ⇒ Single key is shared by all users 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.
 - ⇒ Can use different keys in two directions.
- ❑ Base key is combined with a 24-bit initialization vector (IV)
 - ⇒ 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



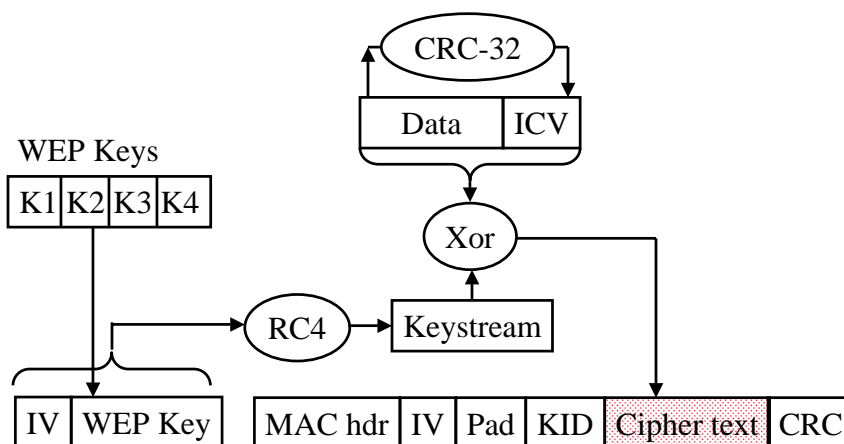
Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-7

WEP Encapsulation



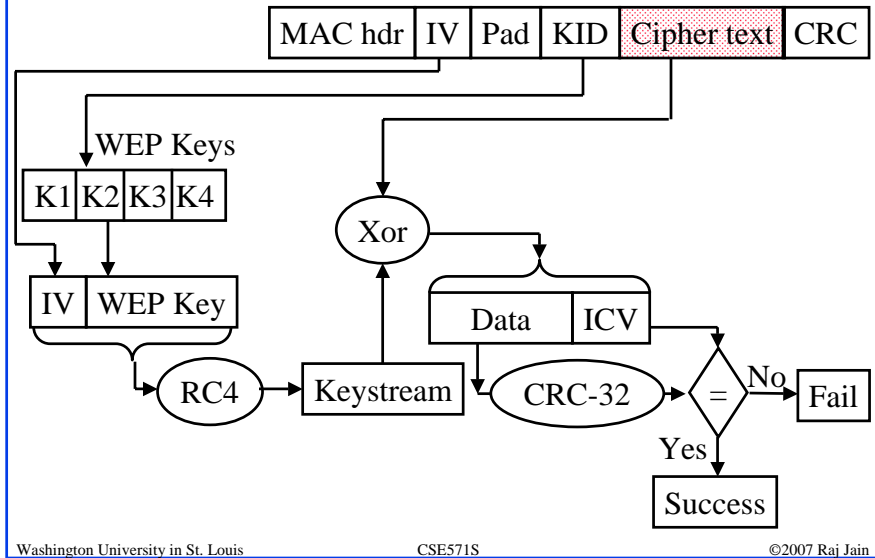
Washington University in St. Louis

CSE571S

©2007 Raj Jain

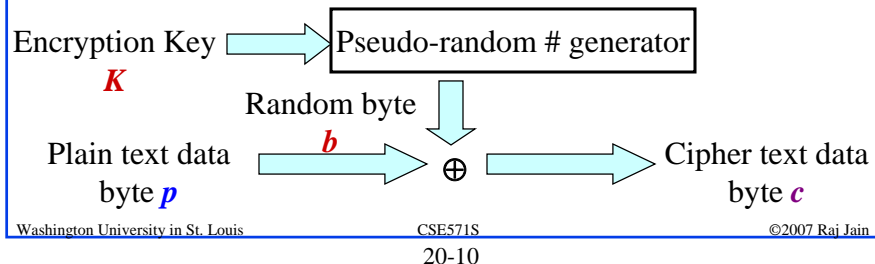
20-8

WEP Decapsulation



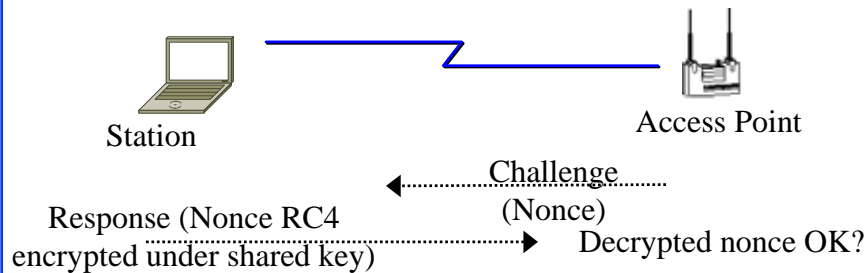
Ron's Cipher 4 (RC4)

- ❑ 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.

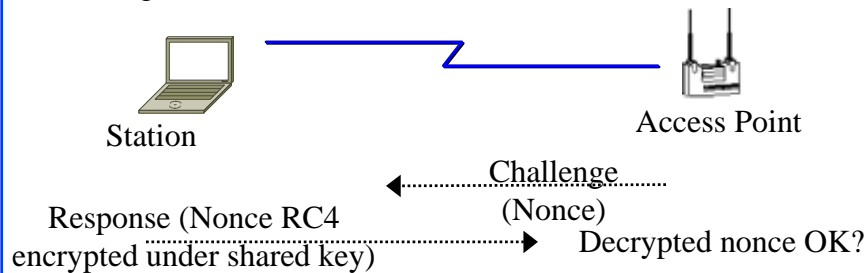


WEP Review

- ❑ 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 \mathbf{b}
- ❑ $\mathbf{c1} = \mathbf{p1} \oplus \mathbf{b}$; $\mathbf{c2} = \mathbf{p2} \oplus \mathbf{b} \Rightarrow \mathbf{c1} \oplus \mathbf{c2} = \mathbf{p1} \oplus \mathbf{p2}$
- ❑ 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
$$\mathbf{p} = p_n x^n + p_{n-1} x^{n-1} + \dots + p_0 x^0$$
- ❑ Remainder($\mathbf{p}+\mathbf{q}$, c)
= Remainder(\mathbf{p} , c) + Remainder(\mathbf{q} , c)
- ❑ ICV is linear: ICV($\mathbf{p}+\mathbf{q}$) = ICV(\mathbf{p}) + ICV(\mathbf{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 \Rightarrow Difficult to change keys
- ❑ Single set of Keys shared by all \Rightarrow 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
- ❑ <http://Netstumbler.com> has on-line database
- ❑ Also, **Warstrolling** and **Warflying**
- ❑ **Warchalking**: Signposting open access on sidewalk or wall
- ❑ Ref: <http://www.warchalking.org>



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>
- ❑ Wellenreiter, <http://www.wellenreiter.net>
- ❑ Mac Stumbler, www.macstumbler.com for Macs
- ❑ KisMAC, www.binaervarianz.de/projekte/programmineren/kismac
- ❑ BSD Airtools: A set of free BSD tools for FreeBSD
 - ❑ dstumbler for wardriving - w GPS interface
 - ❑ www.dachb0den.com/projects/bsd-airtools.html
 - ❑ Bootable CD from www.warbsd.com

Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-19

Network Stumbler

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



Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-20

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
⇒ for WEP key finding

Wireless Sniffing Tools

Public Domain:

- ❑ Airtsnort (Linux / BSD?), <http://airsnort.shmoo.com>
- ❑ Airosniff (FreeBSD),
<http://gravitino.net/~bind/code/airosniff/>
- ❑ APsniff (Windows),
<http://www.bretmounet.com/ApSniff/index.asp>
- ❑ Aerosol (Windows), <http://www.sec33.com/sniph/aerosol.php>
- ❑ Mognet (Java/Linux), <http://chocobospore.org/mognet/>
- ❑ Kismet (Linux), <http://www.kismetwireless.net/>
- ❑ Prism2Dump (*BSD),
<http://www.dachb0den.com/projects/bsd-airtools.html>
- ❑ Prism Dump, <http://developer.axis.com/software/tools/>
- ❑ Wellenreiter, <http://www.remote-exploit.org/projects.php>



Wireless Sniffing Tools (Cont)

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

Commercial:

- ❑ Airopeek, <http://www.wildpackets.com/products/airopeek>
- ❑ AP Scanner (Mac), <http://homepage.mac.com/typexi/Personal1.html>
- ❑ Grasshopper, <http://www.bvsystems.com/Products/WLAN/Grasshopper/grasshopper.htm> - handheld wireless receiver
- ❑ Sniffer Wireless, www.networkgeneral.com
- ❑ Wireless Snif, www.ufasoft.com/sniffer/

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

Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-23

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

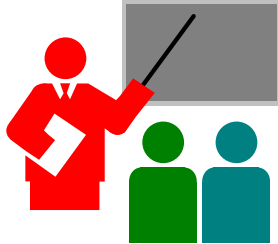
Washington University in St. Louis

CSE571S

©2007 Raj Jain

20-24

Summary



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

References

- ❑ 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
- ❑ A. A. Vladimirov, K.V. Gavrilenko, and A.A. Mikhailovsky, "Wi-Foo: The Secrets of Wireless Hacking," Addison-Wesley, 2004, 560 pp., ISBN:0321202171