Introduction to WiFi Security

Frank Sweetser
WPI Network Operations and Security
fs@wpi.edu

Why should I care?

Or, more formally – what are the risks?

- Unauthorized connections
  - Stealing bandwidth
  - Attacks on your systems from inside firewall
  - Attacks on 3rd party systems that appear to be from you!
- Information leakage
  - Eavesdroppers capturing sensitive information
  - Often can be done from greater range than normal

Typical Options

There are three basic strategies:

- Leave WiFi wide open, roll with whatever comes
- Leave WiFi open, secure it further upstream and/or on a higher level
- Secure the WiFi layer itself

Open Strategy

- Leave your SSID wide open and completely unsecured – very generous of you!
- Be prepared for the repercussions:
  - Attackers and virus infested machines
  - Accusations of bad things other connected users did
- If popular, you may not have any bandwidth left over!

Open WiFi, Secure Upstream

- Treat WiFi as insecure link – think Internet
- Any WiFi facing hosts must be thoroughly secured bastion hosts
- *Any* leaks will allow users to bypass filters
  - ping
  - DNS
  - Web
- nocat.net
- OpenVPN.org

Securing WiFi

- Create Access Control Lists
- Make it invisible
- Encryption

MAC Address Filtering

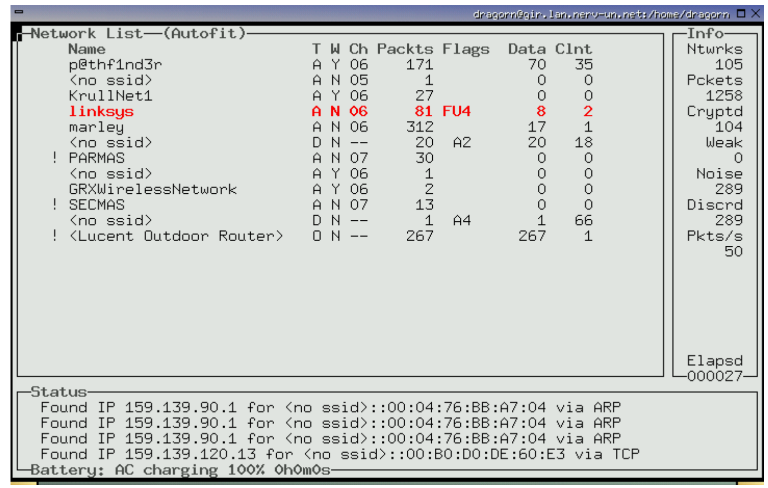
- Commonly available and suggested choice
- Very weak – trivially spoofable, even in Windows!
- Only useful for preventing accidental associations from ignorant bystanders

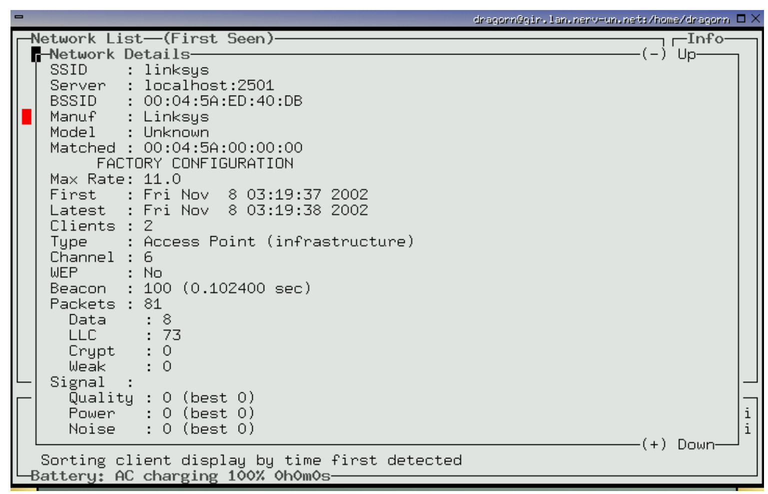
Hidden SSID

- Many APs allow you to remove the SSID from the beacons
- Makes network invisible, right?
- Significantly longer roaming times – very bad if you're running VoIP over WiFi
- SSID still present in other frames
- Enter kismet...

Kismet Wireless Monitor

- Linux based passive wireless sniffer
- Monitors all packets, not just beacons
- Can find hidden networks
- Supports GPS
- Pulls tons of other useful/dangerous information





Kismet with GPS Daemon

Native WiFi Security and Encryption

- Past Mistakes
  - Original Wired Equivalent Privacy (WEP)
- Modern Encryption
  - WiFi Protected Access (WPA)
  - Robust Secure Network (RSN/802.11i/WPA2)
- Authentication
  - Shared Key
  - 802.1x and RADIUS

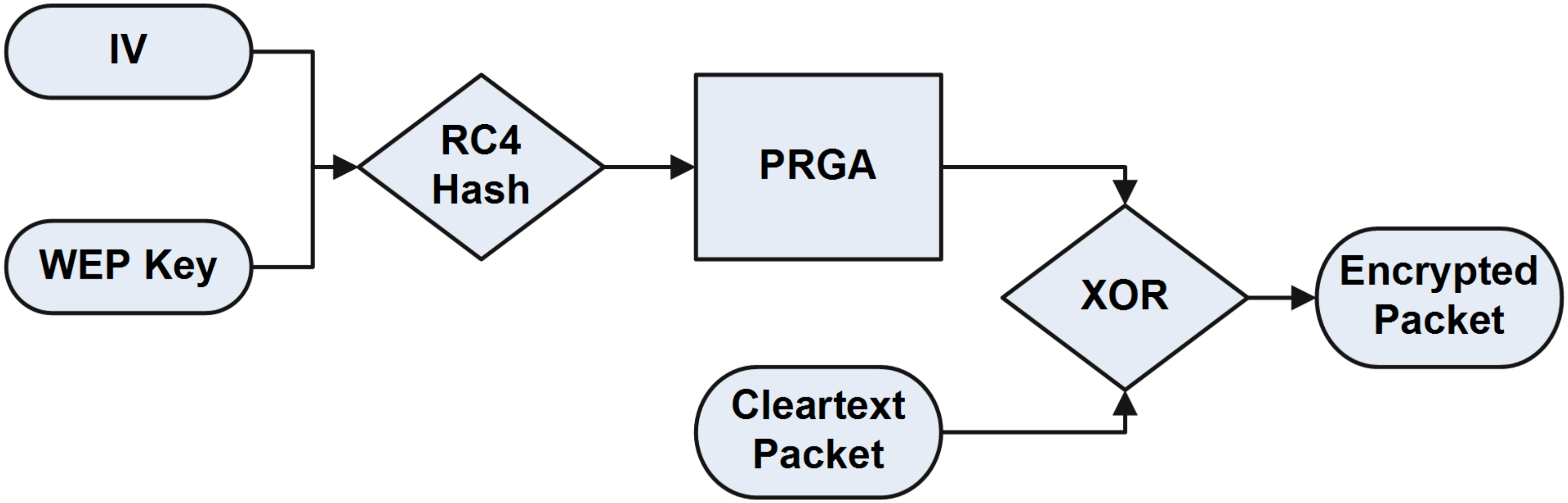
WEP

- Originally developed by IEEE in 1997
- Meant only to provide about same privacy as using a cable – i.e., not much
- Uses RC4 encryption – simple, fast, easily implemented in cheap hardware
- Numerous vulnerabilities in all stages

WEP Encryption Keys

- WEP Security provided by 40 or 104 bit static pre-shared key
- 24 bit per-packet Initialization Vector (IV) transmitted with each packet
- IV is appended to static key for encryption/decryption, giving the 64 or 128 bits marketing likes to talk about

WEP Encryption Engine (Simplified)



Swap Cleartext and Encrypted packets for decryption

XOR

- A XOR B is true if only one of A or B is true

  0 XOR 0 = 0 1 XOR 0 = 1

  1 XOR 1 = 0 0 XOR 1 = 1

- For A XOR B = C, given any two of A, B, or C, the third can be found!

  A XOR B = C

  B XOR C = A

  A XOR C = B

WEP Authentication

- AP Sends random challenge to client
- Client uses key to create PRGA, XORs with random challenge
- XORd challenge sent to AP to prove possession of key
- Attacker can XOR challenge and response to recreate PRGA
- Attacker can now pass authentication without knowing shared key!

IV Reuse

- Multiple instances of the same IV on different packets will eventually allow shared key to be recovered
- 24 bit IV only allows for 16,777,216 values
- Allows for 16k IVs for *all nodes* using shared key for the *entire lifetime* of the key
- In other words, IV reuse is
  - Very bad for security
  - Inevitable, especially on a large network

Direct Attacks on Shared Key

- FMS attacks provided reliable method of recovering shared key from traffic analysis
- Certain “weak” IV values leak bits of key
  - IV of pattern a:FF:b leaks byte a-3 of key
  - Many other weak patterns found since
- Skipping weak values to avoid direct attacks only helps statistical attacks
- Still takes thousands of captured packets

No Replay Protection

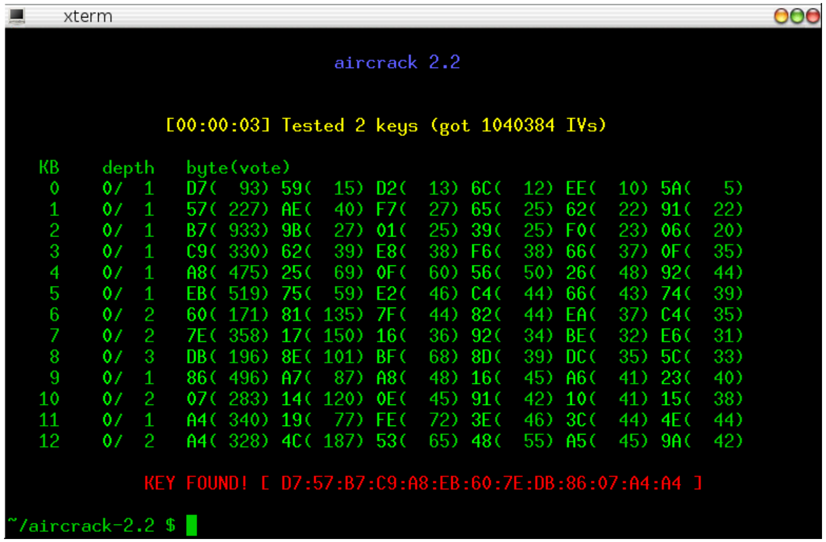
- Attacker gathers few hundred encrypted packets
- Attacker retransmits each one, until one that generates response is found (ping, ARP, SYN packet, etc)
- Once response generator is found, attacker floods it until enough packets to crack key are generated
- aireplay (part of aircrack) can pick likely ARP requests from capture file and replay automatically

Packet Injection

- Remember PRGA trick from shared key authentication?
- No secure session authentication
- Same PRGA and IV can be used to generate and inject packets up to 132 bytes long
- Enough to play with stateful firewalls
- WEPWedgie automates packet injection

WEP Attack Tools

- aircrack
- airsnort
- Both tools can reliably recover static WEP keys
- aircrack often effective with as few as 75k packets!
- Once enough traffic is captured, analysis is typically under 1 minute



So Now What?

- IEEE had already begun work on 802.11i with AES to address all known security problems
- After FMS opened floodgates on breaking WEP key, IEEE realized 802.11i and AES hardware was too far off to help
- Took critical parts, adapted to WEP hardware, and released as WPA

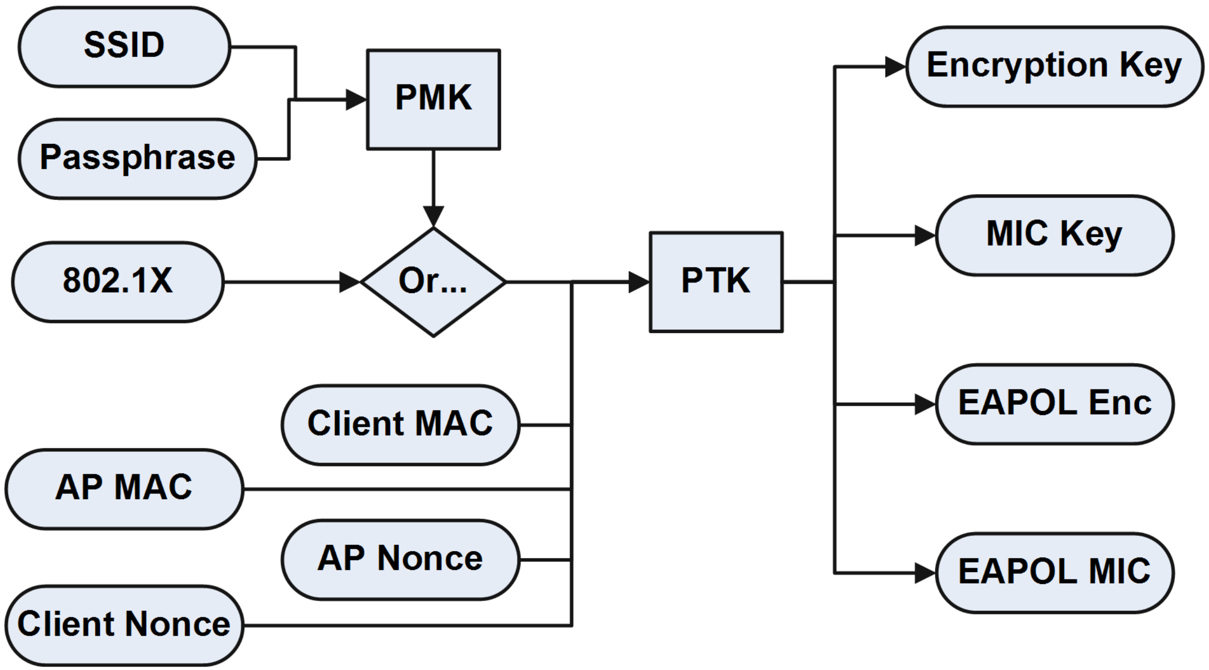
WiFi Protected Access

- Designed explicitly to address WEP vulnerabilities
- Any WEP compatible hardware should also support WPA
- Drivers need updating
- Supports pre-shared key or 802.1x
- Naive WEP RC4 usage algorithm replaced with TKIP

WPA Highlights

- Shared secret is never used directly
- IV reuse no longer possible
- Secure MIC checksum prevents replay/injection
- 4 Way Handshake allows two way authentication

TKIP Key Generation



Impossible to use any final keys for other purpose or recreate original secrets

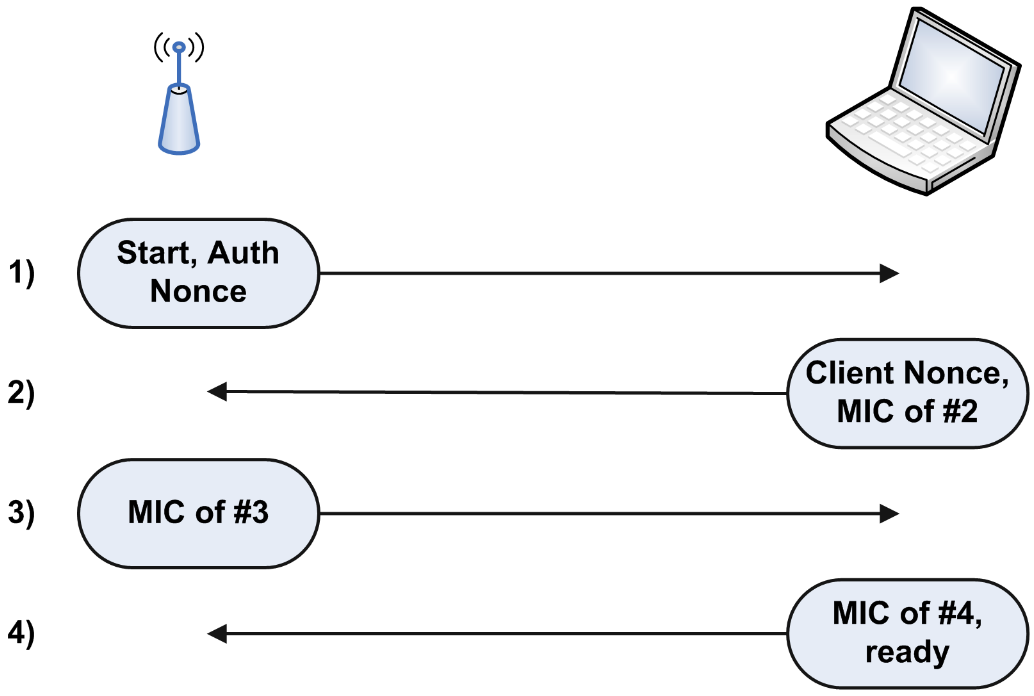
No IV Reuse

- TKIP sequence number increased to 48 bits
- Used to generate 24 bit value for WEP hardware compatibility
- “Weak” IV values that leak key are avoided
- Sequences numbers must
  - Start at 0
  - Increase for each packet sent
  - Be dropped if IV is lower than last one sent

Secure MIC Checksum

- Message Integrity Check
- Calculates 64 bit value based on packet data and PTK generated secret
- Provides ~29 bits of randomness
- In theory, guessable in about 2 minutes at 802.11b data rates
- More than two MIC violations in 60 seconds shuts down radio for 60 seconds

Four Way Handshake



- Nonces plus PMK, MACs create keys
- Both ends safely validate each other

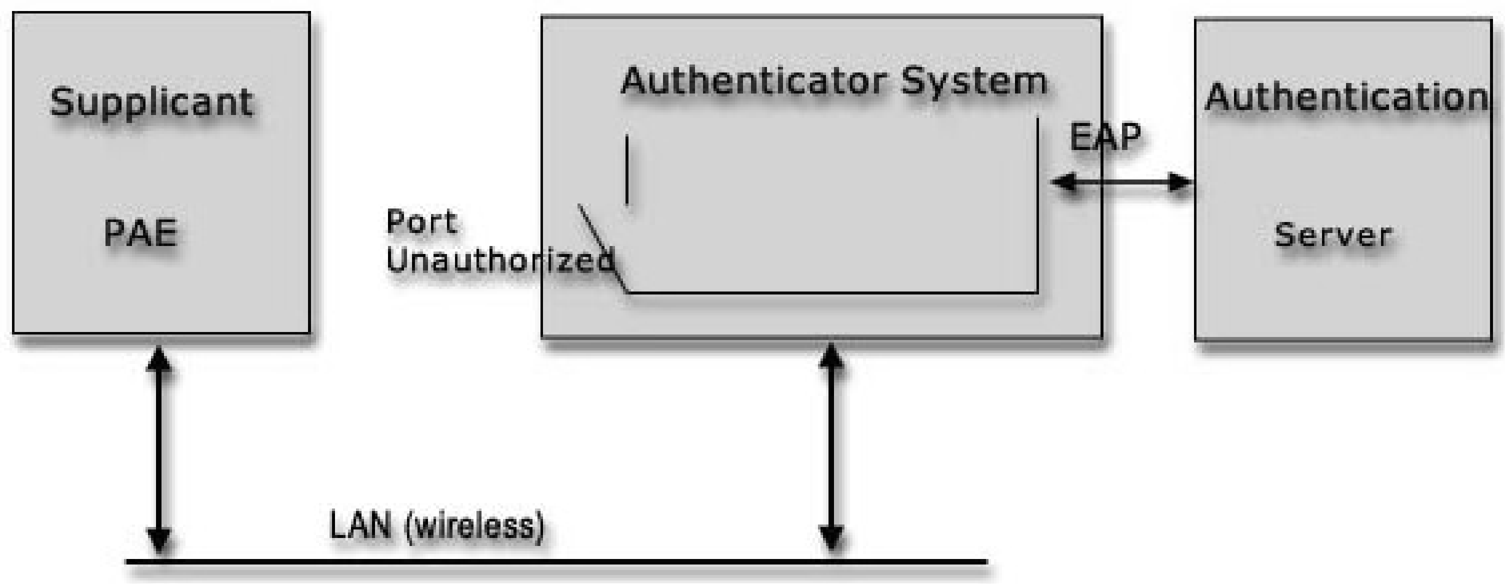
Robust Security Network

- RSN, aka 802.11i, aka WPA2
- Served as the model for WPA
- Requires AES support in hardware
- Operationally nearly identical to WPA

802.1x

- Uses RADIUS backend to securely authenticate connecting machines
- Numerous different authentication types
  - MS-CHAP, TLS, PEAP, etc
- Can also be used to seed and rotate encryption engines instead of static shared secret
- Most dynamic WEP implementations are broken and don’t rotate keys!
- The “Enterprise” part of WPA-Enterprise

802.1x Diagram



What About Denial of Service?

- Wireless is an inherently shared medium
- Several protocol level DoS attacks
  - Medium reservation
  - Deauth/disassociate flood
- Intentionally not addressed in WPA
- Best encryption in the world can’t trump raw 2.5/5.8Ghz noise

Summary

- WEP just gives false sense of security
- Open WiFi secured upstream possible, but difficult
- WPA-PSK commonly available, gives very good security
- Questions? Comments? Suggestions?

Resources

- Kismet

  http://www.kismetwireless.net/
- airodump, aircrack

  http://www.wirelessdefence.org/Contents/Aircrack_airodump.htm
- Back Track bootable wireless/security auditing

  http://www.remote-exploit.org
- Fluhrer, Mantin, Shamir WEP Weakness

  http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- Linux wpa supplicant

  http://hostap.epitest.fi/wpa_supplicant
- Real 802.11 Security

  Edney, Arbaugh ISBN 0-321-13620-9