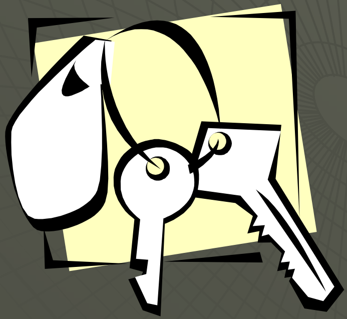
WLAN and IEEE 802.11 Security



Atin Kumar
Puja Thakral
Soumya Das

Agenda

- Intro to WLAN
- Security mechanisms in IEEE 802.11
- Attacks on 802.11
- Securing a wireless network
- Future Trends
- Summary

Why WLAN ?

- The major motivation and benefit from wireless LANs is increased mobility.

- Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.

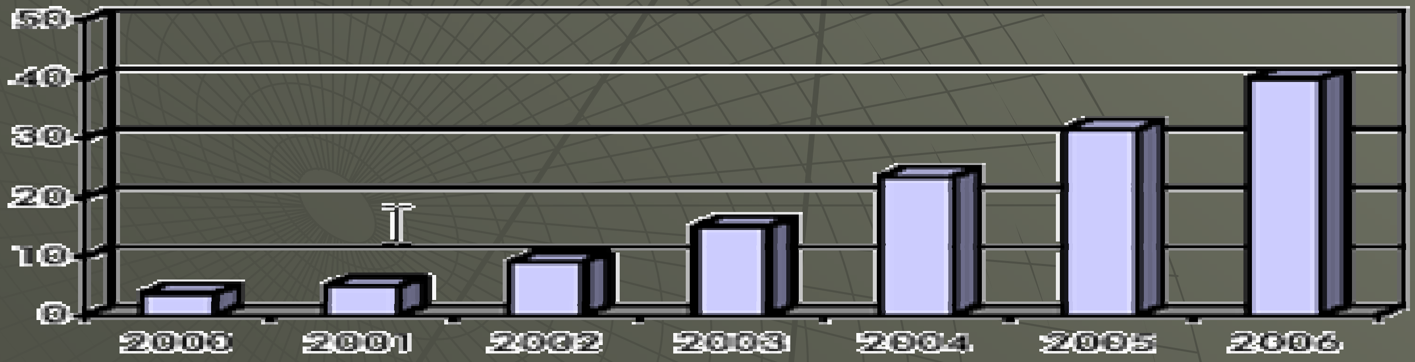
- In addition to increased mobility, wireless LANs offer increased flexibility.

The list is endless…

Wireless LAN Technologies

- IEEE 802.11
- HiperLAN
- Bluetooth

WLAN End User Forecast (millions)



HiperLAN2

- HiperLAN2

  KEY FEATURES

  - High throughput
  - Up to 54 Mbps (gross)
  - LAN coverage
  - Indoor 30 m radius
  - Outdoor 150 m radius
  - Quality Of Service
  - Supports voice, video and multimedia applications
  - 802.1p and ATM QOS
  - Scalable security
  - 56 bit to 168 bit key encryption (DES)
  - Optional pre shared or public key authentication

Bluetooth

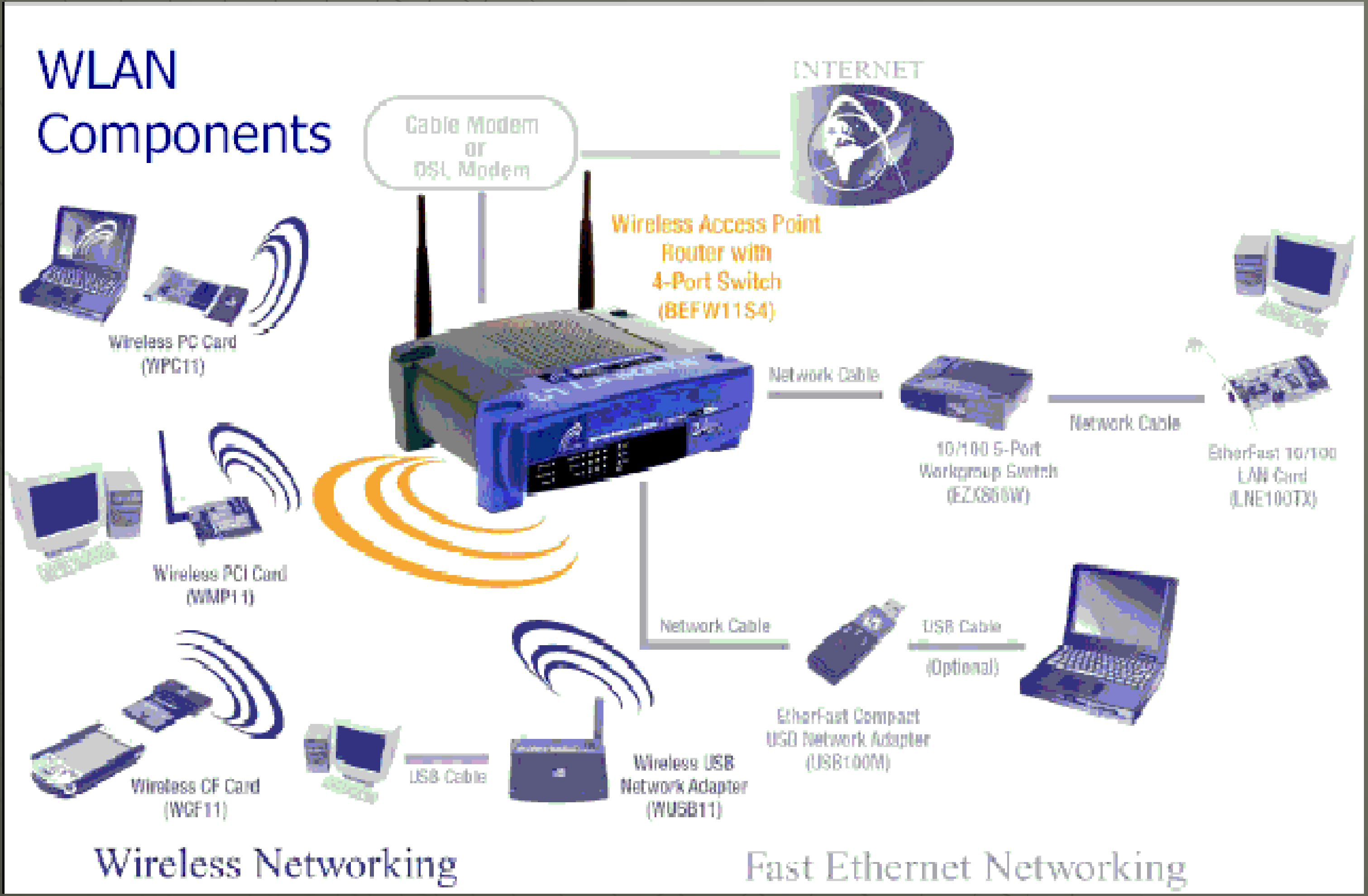
- Cable replacement
- Self-forming PANs (Personal Area Networks)
- Freq: 2.4 GHz band
- Power 1mw to 100 mw
- Mode : FHSS
- Range: 40-50 Feet
- Data Rate: Approx 400 Kbps
- Security better than Wi-Fi but not MUCH of a concern.

What is an IEEE 802.11 Wireless Network ?

- Speeds of upto 54 Mb/s
- Operating Range: 10-100m indoors, 300m outdoors
- Power Output Limited to 1 Watt in U.S.
- Frequency Hopping (FHSS), Direct Sequence
- (DSSS), & Infrared (IrDA)

  (– Networks are NOT compatible with each other)
- Uses unlicensed 2.4/5 GHz band (2.402-2.480 ,5 GHz)
- Provide wireless Ethernet for wired networks

WLAN Components

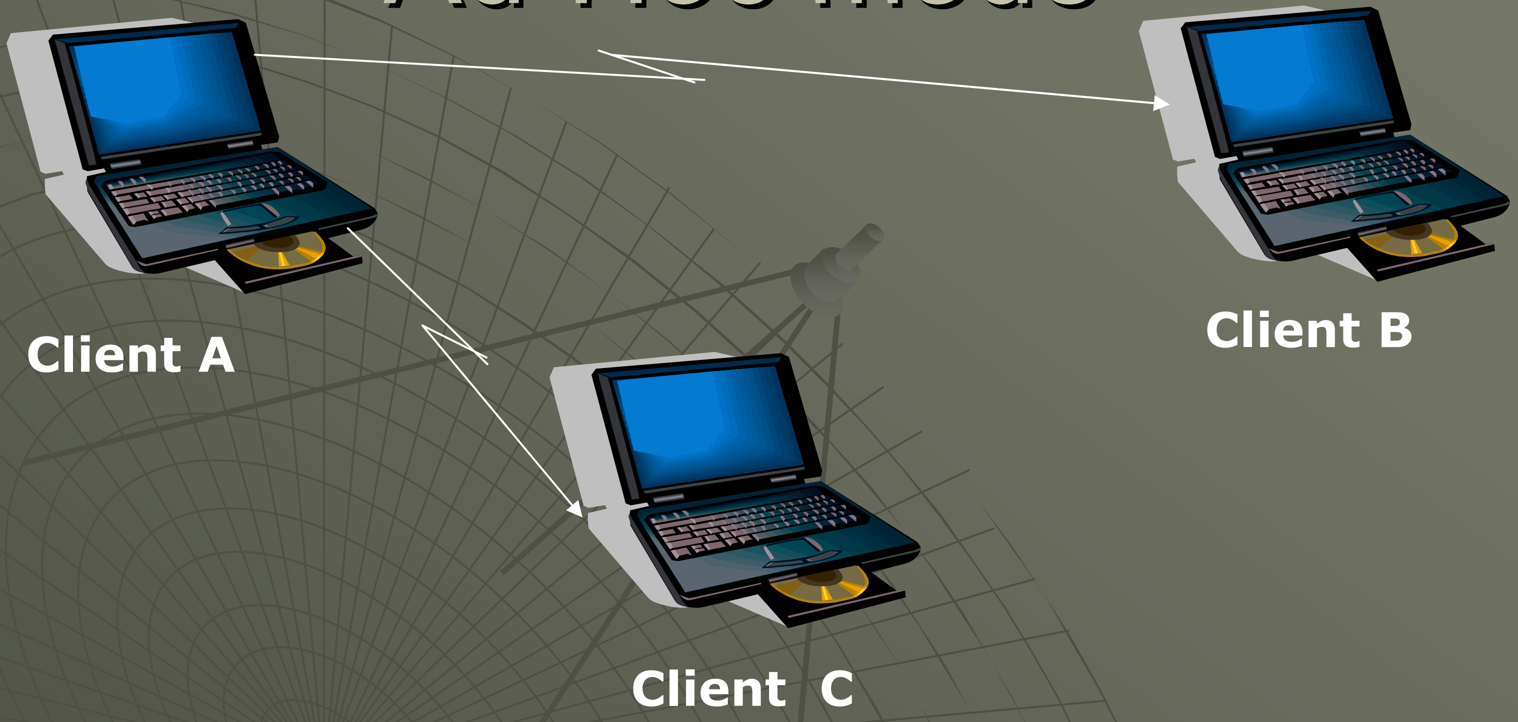

WLAN Components
INTERNET
Cable Modem or DSL Modem
Wireless Access Point Router with 4-Port Switch (BEFW11S4)
Wireless PC Card (WPC11)
Network Cable
10/100 5-Port Workgroup Switch (EZXS55W)
Network Cable
EtherFast 10/100 LAN Card (LNE100TX)
Wireless PCI Card (WMP11)
Network Cable
USB Cable
(Optional)
EtherFast Compact USB Network Adapter (USB100M)
Wireless CF Card (WCF11)
USB Cable
Wireless USB Network Adapter (WUSB11)
Wireless Networking
Fast Ethernet Networking

More about WLAN

Modes of Operation

- Ad-Hoc mode (Independent Basic Service Set - IBSS)
- Infrastructure mode (Basic Service Set - BSS)

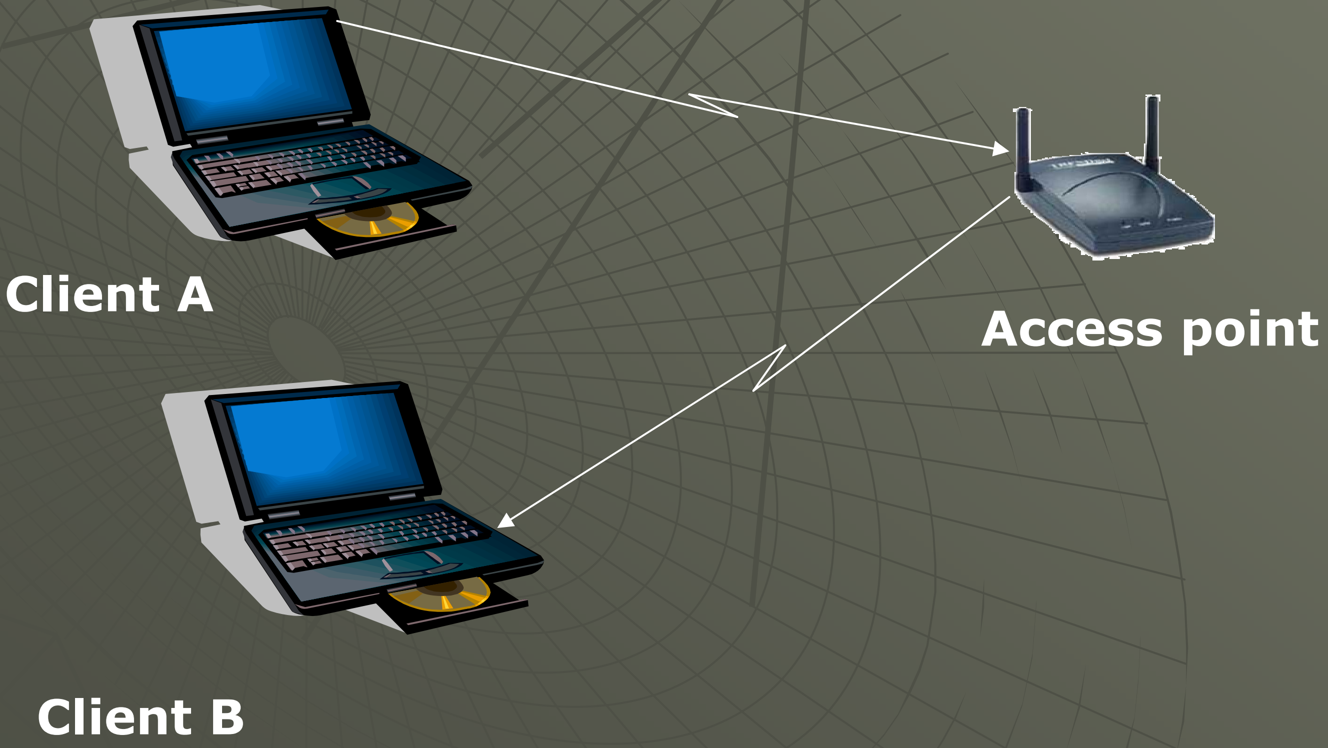
Ad-Hoc mode



Laptop users wishing to share files could set up an ad-hoc network using 802.11 compatible NICs and share files without need for external media eg. floppy disks.

Infrastructure mode

In this mode the clients communicate via a central station called Access Point (AP) which acts as an ethernet bridge and forwards the communication onto the appropriate network, either the wired or the wireless network.



Client A

Access point

Client B

The Chain of Trust

Authentication

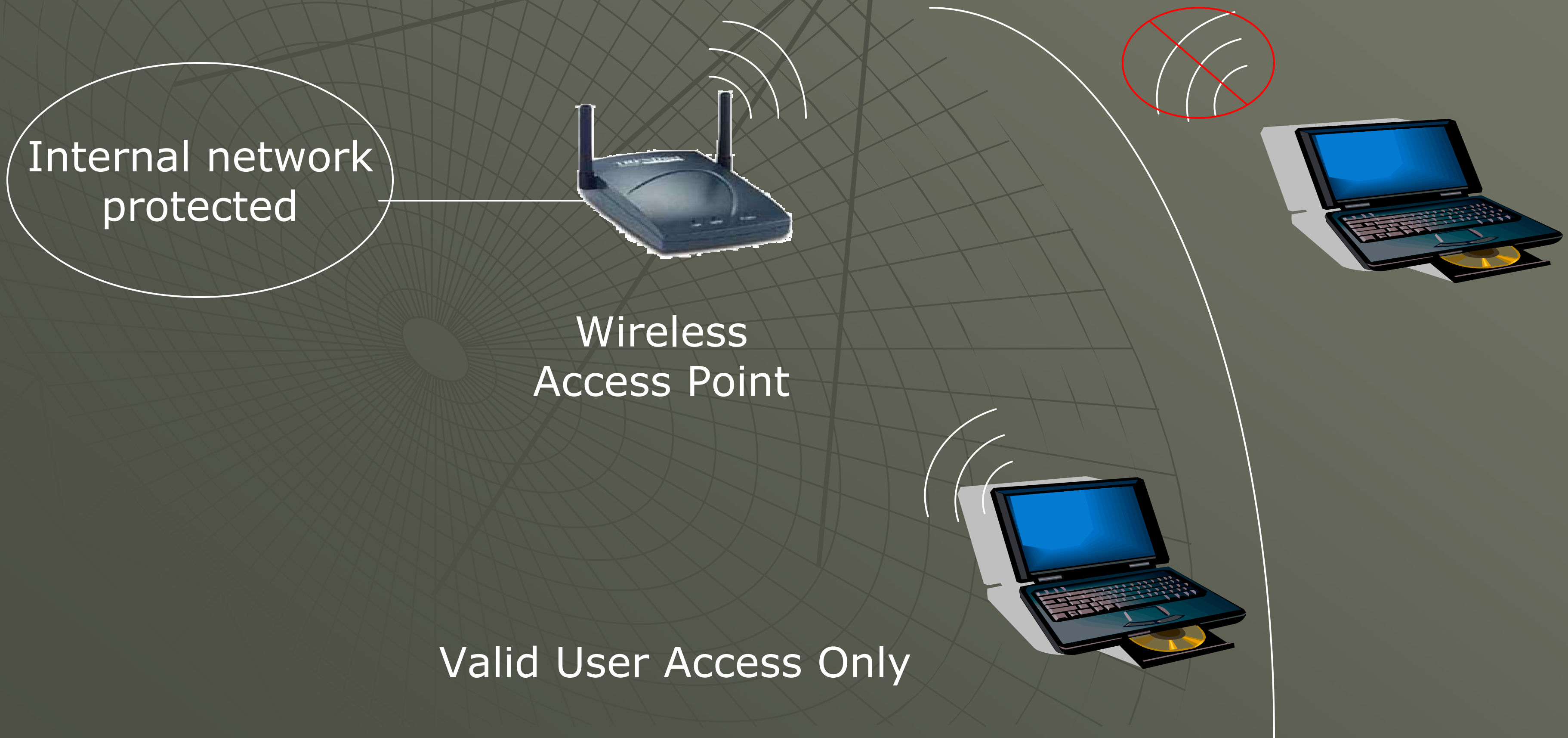
Authorization

Data Integrity

Data Confidentiality

WLAN security – Problem !!

There is no physical link between the nodes of a wireless network, the nodes transmit over the air and hence anyone within the radio range can eavesdrop on the communication. So conventional security measures that apply to a wired network do not work in this case.



Internal network protected

Wireless Access Point

Valid User Access Only

IEEE 802.11 basic security mechanisms

- Service Set Identifier (SSID)
- MAC Address filtering
- Open System Authentication
- Shared Key Authentication
- Wired Equivalent Privacy (WEP) protocol

802.11 products are shipped by the vendors with all security mechanisms disabled !!

Service Set Identifier (SSID)

- Limits access by identifying the service area covered by the access points.

- AP periodically broadcasts SSID in a beacon.

- End station listens to these broadcasts and choose an AP to associate with based upon its SSID.

SSIDs are “useless”!

- Use of SSID – weak form of security as beacon management frames on 802.11 WLAN are always sent in the clear.
- A hacker can use analysis tools (eg. AirMagnet, Netstumbler, AiroPeek) to identify SSID.
- Some vendors use default SSIDs which are pretty well known (eg. CISCO uses tsunami)

MAC Address Filtering

The system administrator can specify a list of MAC addresses that can communicate through an access point.

Advantage :

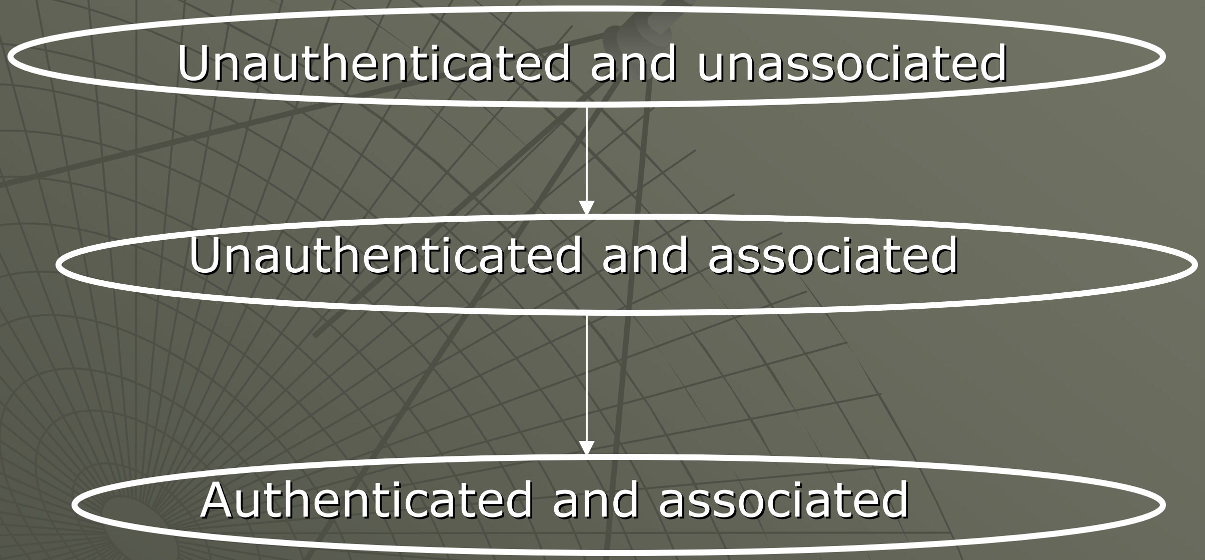
- Provides stronger security than SSID

Disadvantages :

- Increases Administrative overhead
- Reduces Scalability
- Determined hackers can still break it

Association and Authentication

The association process is a two-step process involving three states:



Unauthenticated and unassociated

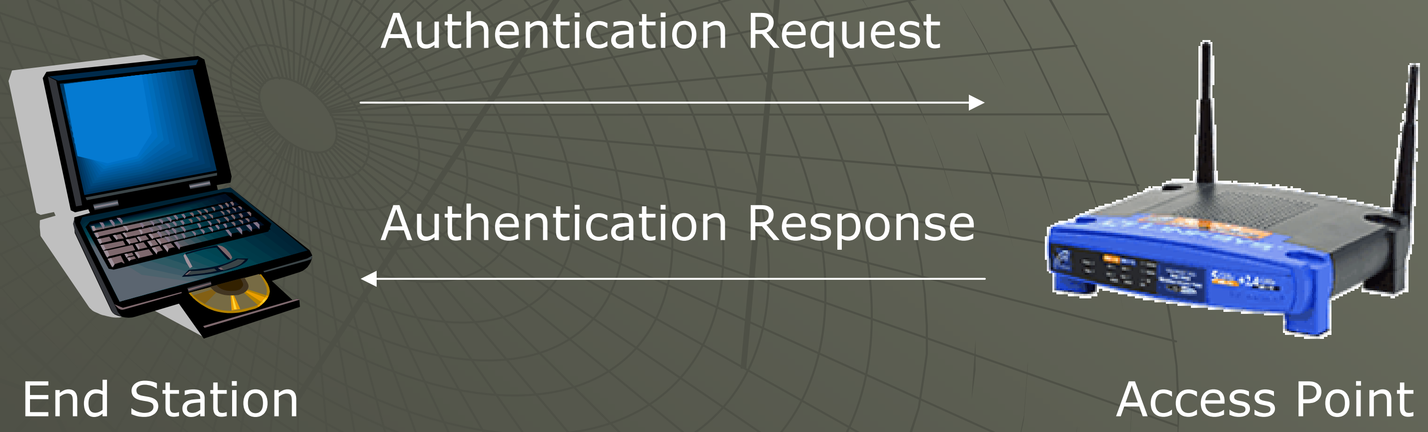
Unauthenticated and associated

Authenticated and associated

To transition between these states the communicating parties exchange messages called management frames.

Open System Authentication

- The default authentication protocol for 802.11.
- Authenticates anyone who requests authentication (null authentication).



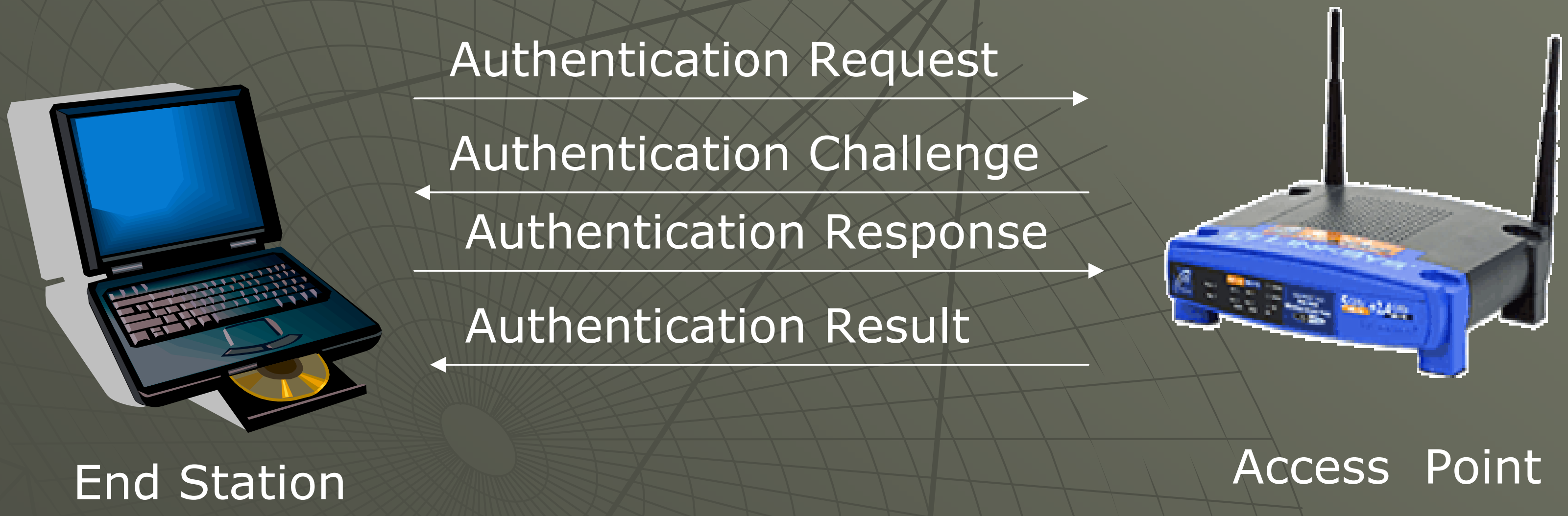
Authentication Request

Authentication Response

End Station

Access Point

Shared Key Authentication



Authentication Request

Authentication Challenge

Authentication Response

Authentication Result

End Station

Access Point

Open System Vs Shared Key Authentications

- Shared Key Authentication is never recommended!

- Better to use Open System Authentication, which allows authentication without the correct WEP key.

Wired Equivalent Privacy (WEP)

- Designed to provide confidentiality to a wireless network similar to that of standard LANs.

- WEP is essentially the RC4 symmetric key cryptographic algorithm (same key for encrypting and decrypting).

WEP Contd..

- Transmitting station concatenates 40 bit key with a 24 bit Initialization Vector (IV) to produce pseudorandom key stream.
- Plaintext is XORed with the pseudorandom key stream to produce ciphertext.
- Ciphertext is concatenated with IV and transmitted over the Wireless Medium.
- Receiving station reads the IV, concatenates it with the secret key to produce local copy of the pseudorandom key stream.
- Received ciphertext is XORed with the key stream generated to get back the plaintext.

WEP has its cost!

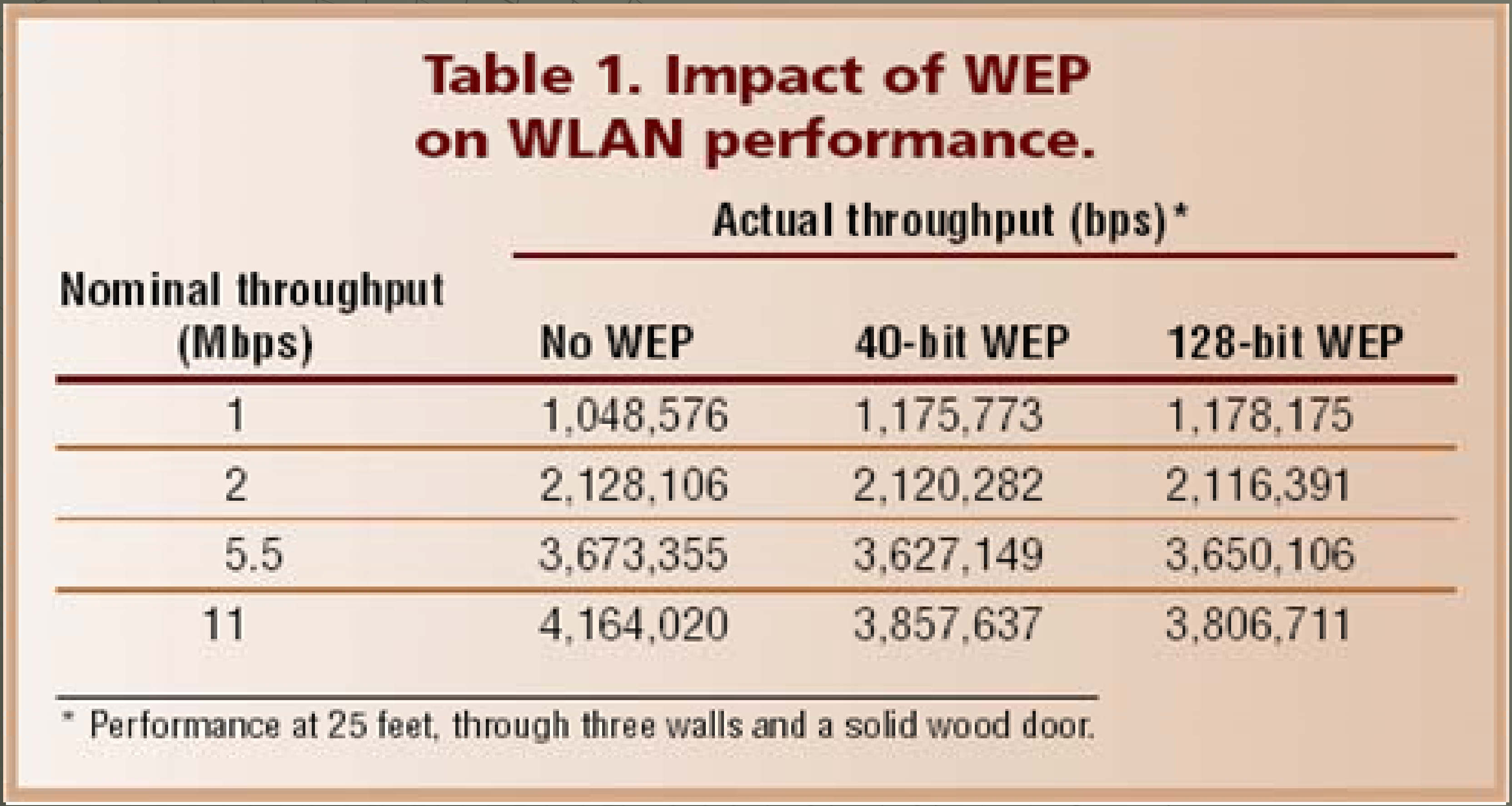


Table 1. Impact of WEP on WLAN performance.

	Actual throughput (bps)*		
Nominal throughput (Mbps)	No WEP	40-bit WEP	128-bit WEP
1	1,048,576	1,175,773	1,178,175
2	2,128,106	2,120,282	2,116,391
5.5	3,673,355	3,627,149	3,650,106
11	4,164,020	3,857,637	3,806,711

* Performance at 25 feet, through three walls and a solid wood door.

WEP – vulnerability to attack

- WEP has been broken! Walker (Oct 2000), Borisov et. al. (Jan 2001), Fluhrer-Mantin -Shamir (Aug 2001).

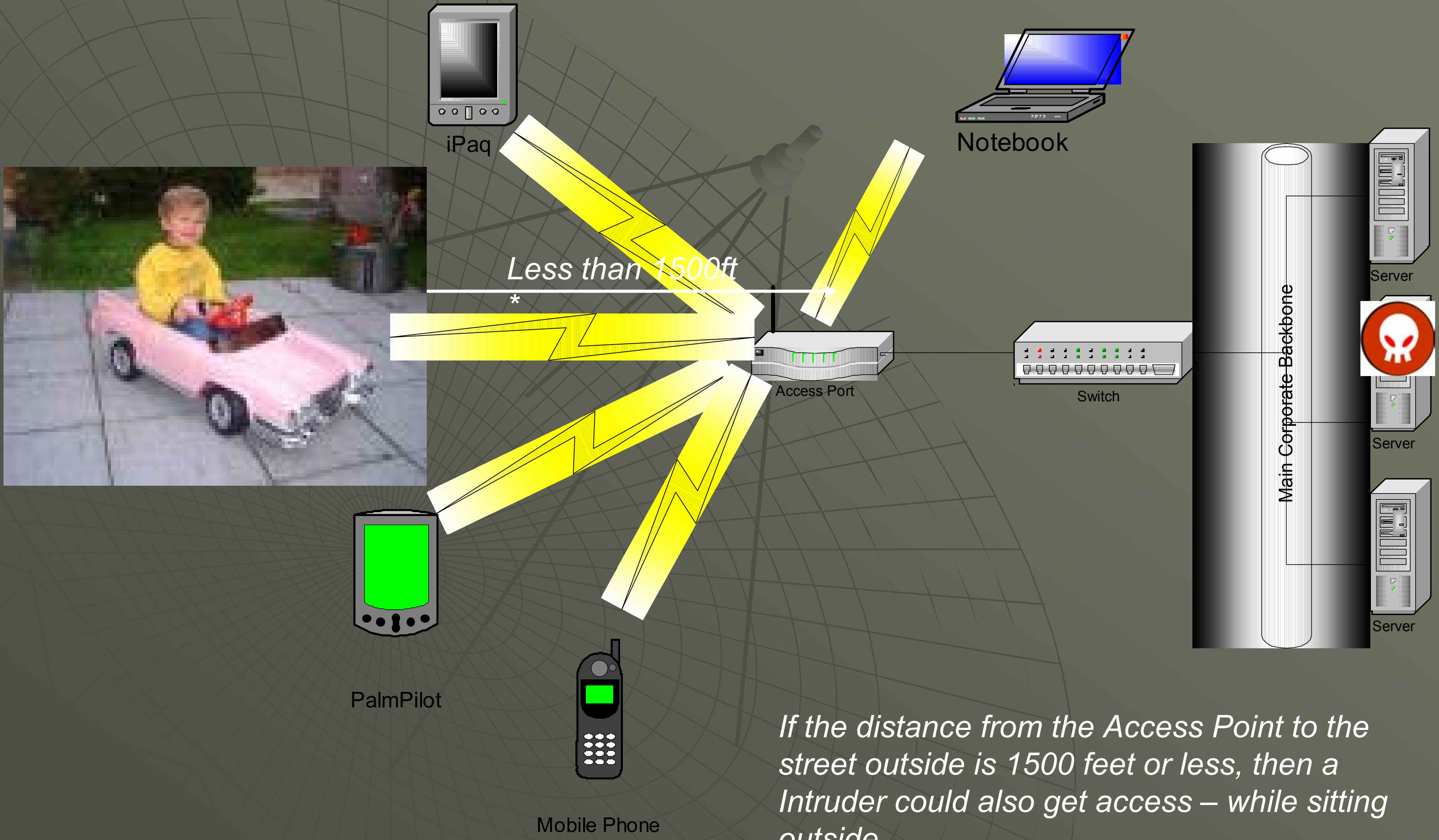
- Unsafe at any key size : Testing reveals WEP encapsulation remains insecure whether its key length is 1 bit or 1000 or any other size.

- More about this at: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

Security Problems of 802.11 Wireless Networks

- Easy Access
- "Rogue" Access Points
- Unauthorized Use of Service
- Traffic Analysis and Eavesdropping
- Higher Level Attacks

"Drive By Hacking"



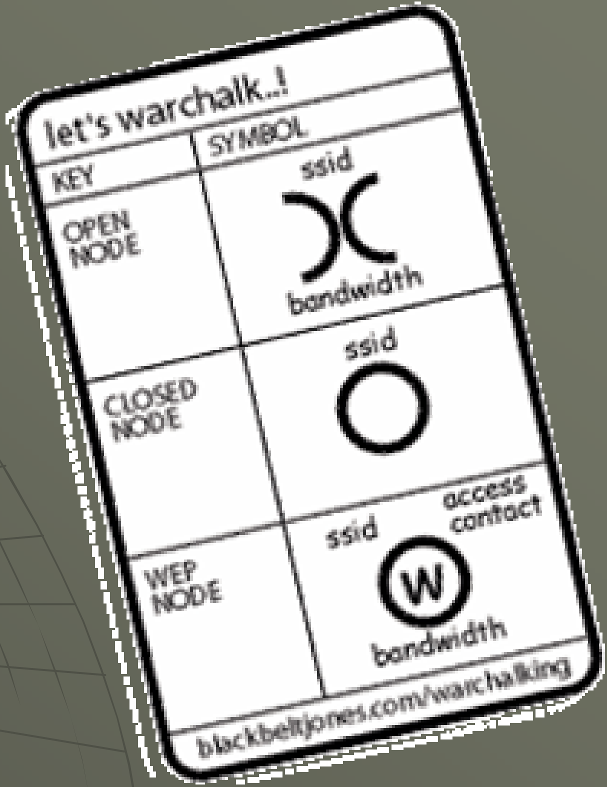
If the distance from the Access Point to the street outside is 1500 feet or less, then a Intruder could also get access – while sitting outside

War-driving expeditions

In one 30-minute journey using the Pringles can antenna, witnessed by BBC News Online, Security company i-sec managed to find and gain information about almost 60 wireless networks.

War Chalking

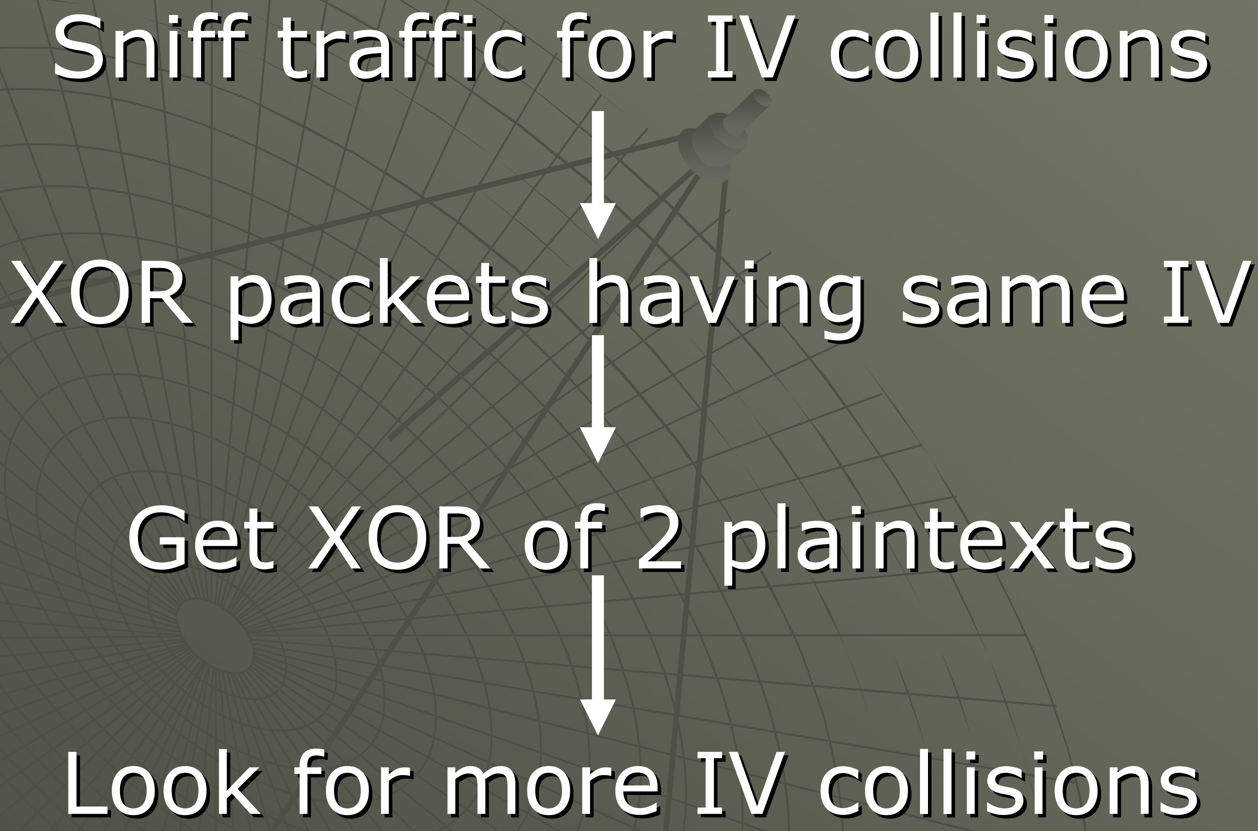
- Practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly.



Types of Attacks

- **Passive Attack to Decrypt Traffic**
- **Active Attack to Inject Traffic**

Passive Attack to Decrypt Traffic



Sniff traffic for IV collisions

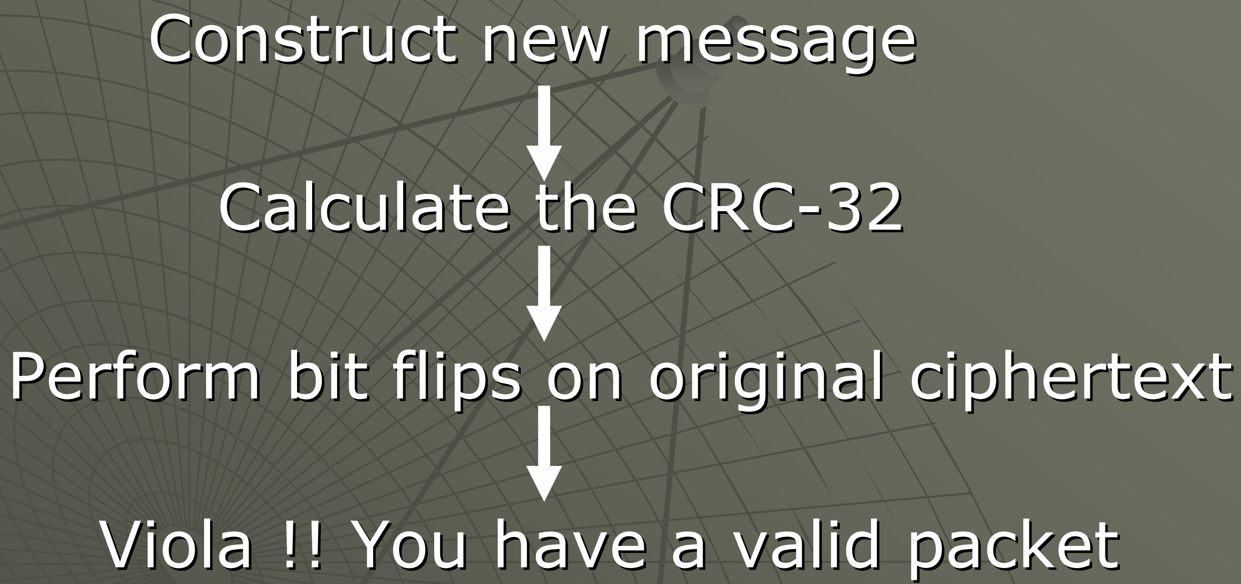
XOR packets having same IV

Get XOR of 2 plaintexts

Look for more IV collisions

Active Attack to Inject Traffic

Plaintext Known



Construct new message

Calculate the CRC-32

Perform bit flips on original ciphertext

Viola !! You have a valid packet

RC4(X) xor X xor Y = RC4(Y)

What are the major security risks to 802.11b?

- Insertion Attacks
- Interception and monitoring wireless traffic
- Misconfiguration
- Jamming
- Client to Client Attacks

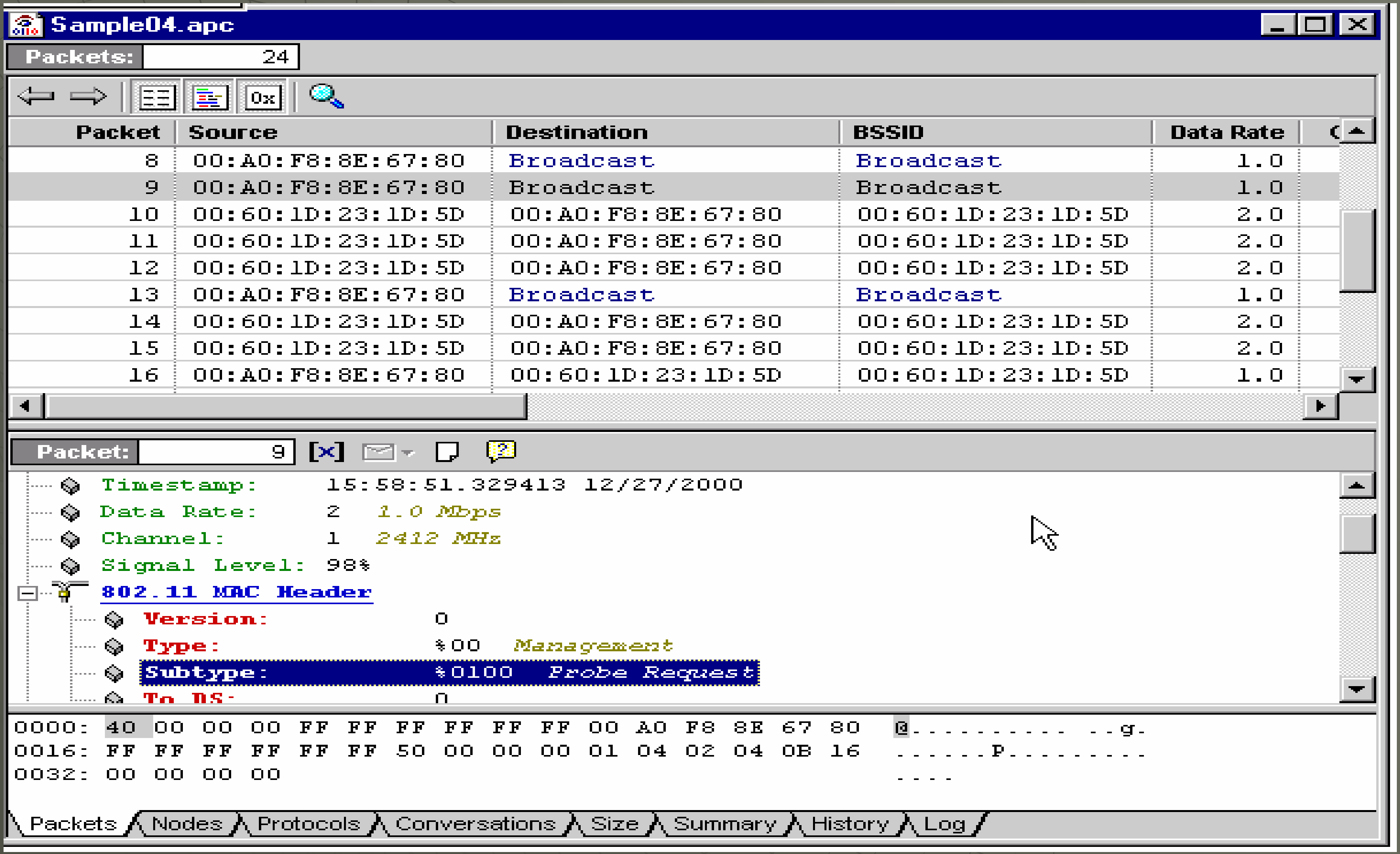
Insertion Attacks

- Plugged-in Unauthorized Clients
- Plugged-in Unauthorized Renegade Base Station

Interception and monitoring wireless traffic attacks

- Wireless Sniffer
- Hijacking the session
- Broadcast Monitoring
- ArpSpoof Monitoring and Hijacking

Packet Sniffing



Sample04.apc

Packets: 24

Packet	Source	Destination	BSSID	Data Rate
8	00:A0:F8:8E:67:80	Broadcast	Broadcast	1.0
9	00:A0:F8:8E:67:80	Broadcast	Broadcast	1.0
10	00:60:1D:23:1D:5D	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	2.0
11	00:60:1D:23:1D:5D	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	2.0
12	00:60:1D:23:1D:5D	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	2.0
13	00:A0:F8:8E:67:80	Broadcast	Broadcast	1.0
14	00:60:1D:23:1D:5D	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	2.0
15	00:60:1D:23:1D:5D	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	2.0
16	00:A0:F8:8E:67:80	00:60:1D:23:1D:5D	00:60:1D:23:1D:5D	1.0

Packet: 9

```
Timestamp:      15:58:51.329413 12/27/2000
Data Rate:      2   1.0 Mbps
Channel:        1   2412 MHz
Signal Level:   98%
802.11 MAC Header
    Version:            0
    Type:               %00     Management
    Subtype:            %0100   Probe Request
    To DS:              0
```

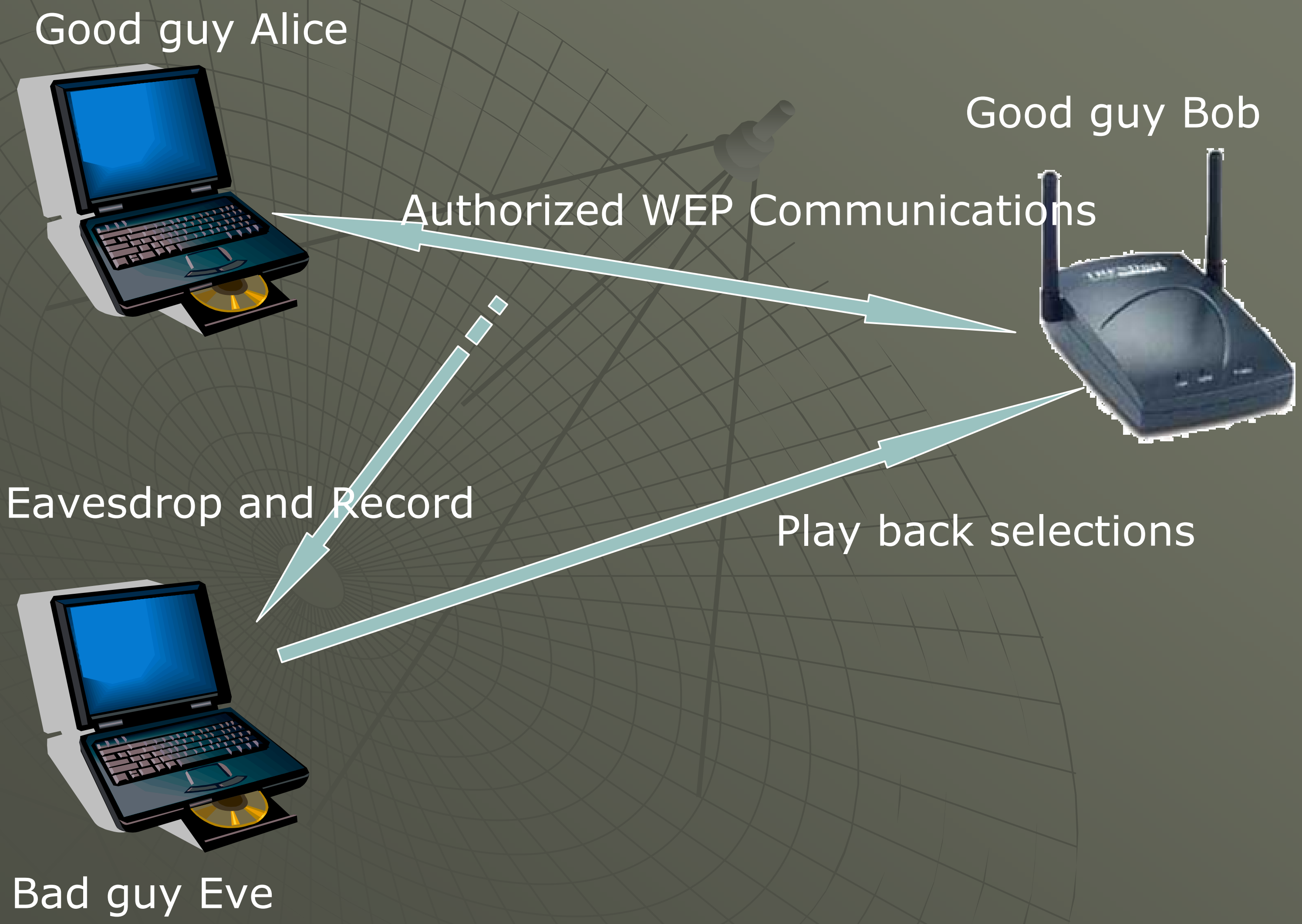
```
0000:  40 00 00 00 FF FF FF FF FF FF 00 A0 F8 8E 67 80   @...........  ..g.
0016:  FF FF FF FF FF FF 50 00 00 00 01 04 02 04 0B 16   ......P.........
0032:  00 00 00 00                                       ....
```

Jamming (Denial of Service)

- Broadcast radio signals at the same frequency as the wireless Ethernet transmitters - 2.4 GHz

- To jam, you just need to broadcast a radio signal at the same frequency but at a higher power.

Replay Attack



Good guy Alice

Good guy Bob

Authorized WEP Communications

Eavesdrop and Record

Play back selections

Bad guy Eve

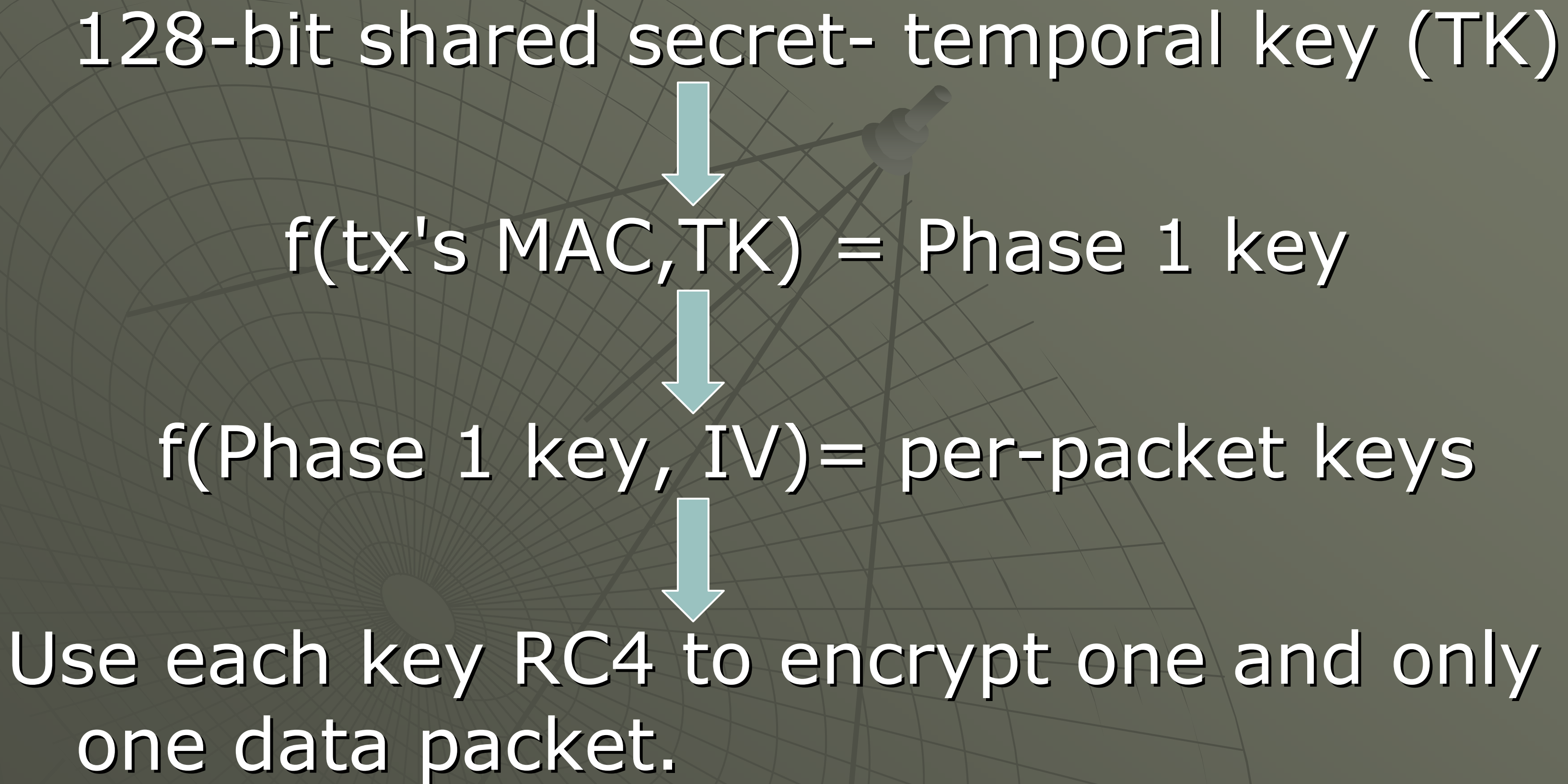
Measures to strengthen WLAN security

Recommendations

Wireless LAN related Configuration

- Enable WEP, use 128bit key*
- Using the encryption technologies
- Disable SSID Broadcasts
- Change default Access Point Name
- No SNMP access
- Choose complex admin password
- Apply Filtering
- Use MAC (hardware) address to restrict access
- SSIDs
- Change default Access Point password
- The Use of 802.1x
- Enable firewall function

TKIP-Enhancement to WEP



128-bit shared secret- temporal key (TK)

f(tx's MAC,TK) = Phase 1 key

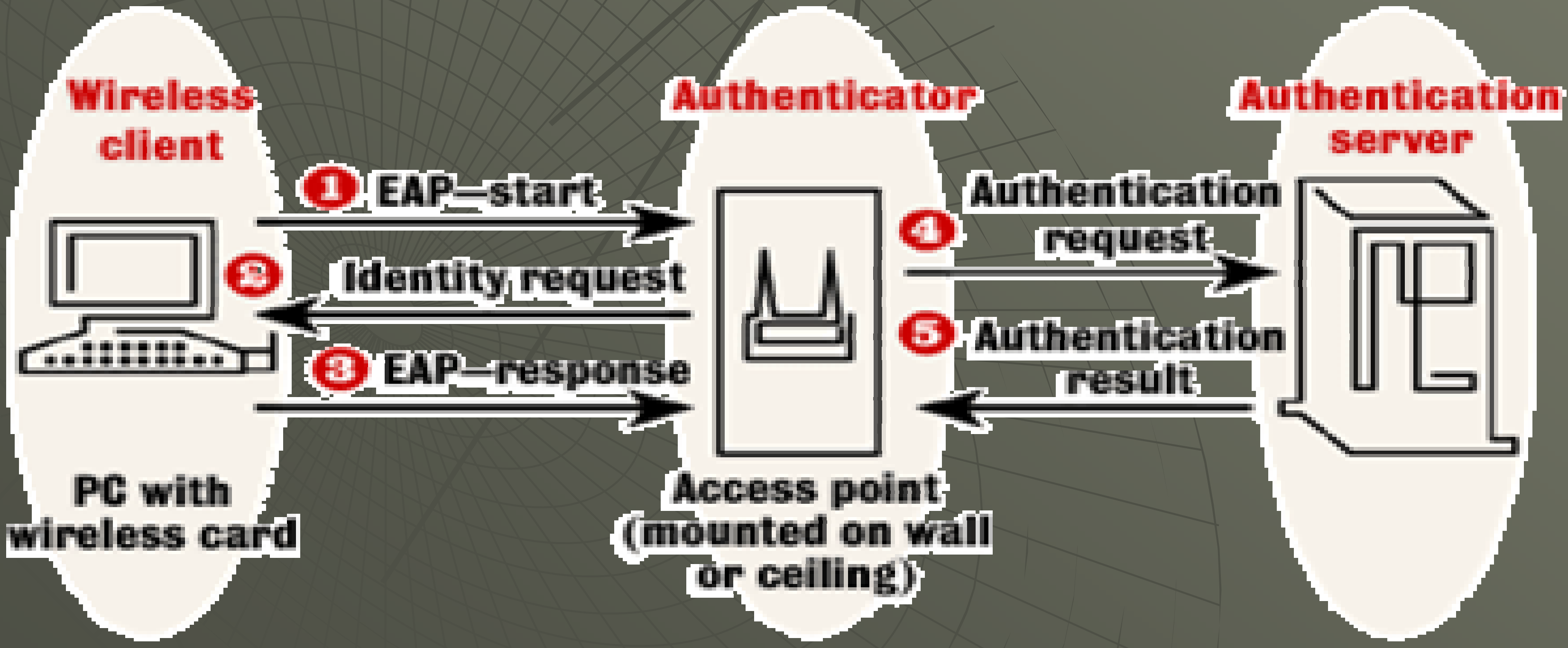
f(Phase 1 key, IV)= per-packet keys

Use each key RC4 to encrypt one and only one data packet.

Future Trends

- Extensible Authentication Protocol (EAP)

The 802.1X standard for port-based authentication and key distribution is based on EAP.



RSN: The Wireless Security Future?

RSN security consists of two basic subsystems:

Data privacy mechanism

- TKIP (a protocol patching WEP)
- AES-based protocol (long term)

Security association management

- RSN negotiation procedures, to establish a security context
- IEEE 802.1X authentication, replacing IEEE 802.11 authentication
- IEEE 802.1X key management, to provide cryptographic keys

802.11i –Secured Wireless

Tentatively called Wi-Fi Protected Access 2 (WPA2) -

- Uses 802.1X, the new IEEE authentication standard
- Replaces WEP with a new standard called Temporal Key Integrity Protocol (TKIP).
- Includes an alternative authentication scheme using a pre-shared key (PSK) methodology for homes and small businesses

Summary

- 802.11 security doesn’t meet any of its security objectives today
- 802.11 TGe is working to replace
  - Authentication scheme using 802.1X and Kerberos
  - Encryption scheme using AES in OCB mode

3 Major Papers on 802.11 Security

- Intercepting Mobile Communications: The Insecurity of 802.11(Borisov, Goldberg, and Wagner 2001)
- Your 802.11 Wireless Network Has No Clothes (Arbaugh, Shankar, and Wan 2001)
- Weaknesses in the Key Scheduling Algorithm of RC4(Fluhrer, Mantin, and Shamir 2001)

Some more References

- The IEEE 802.11b Security Problem, Part 1 (Joseph Williams,2001 IEEE)

- An IEEE 802.11 Wireless LAN Security White Paper (Jason S. King, 2001)

Thank You for Listening

Your feedback as questions or comments is welcome.