WLAN and IEEE 802.11 Security

WIRELESS INFORMATION NETWORK LABORATORY

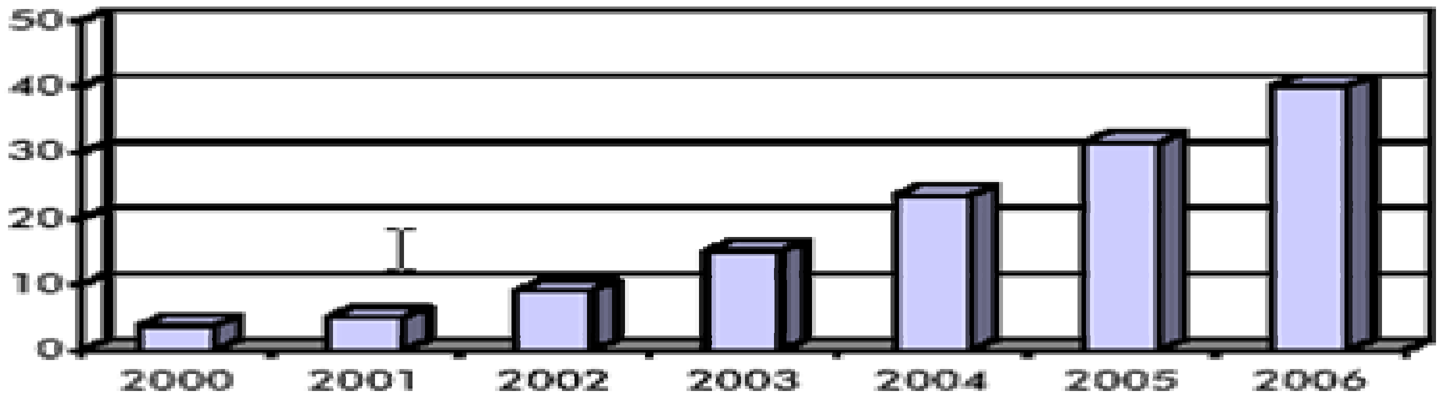
Agenda

- Intro to WLAN
- Security mechanisms in IEEE 802.11
- Attacks on 802.11
- Summary

Wireless LAN Technologies

- WLAN technologies are becoming increasingly popular, and promise to be the platform for many future applications:
  - Home Entertainment Networking
- Example WLAN/WPAN Technologies:
  - IEEE 802.11
  - Bluetooth

WLAN End User Forecast (millions)



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.

- We will not focus on Bluetooth security in this talk.

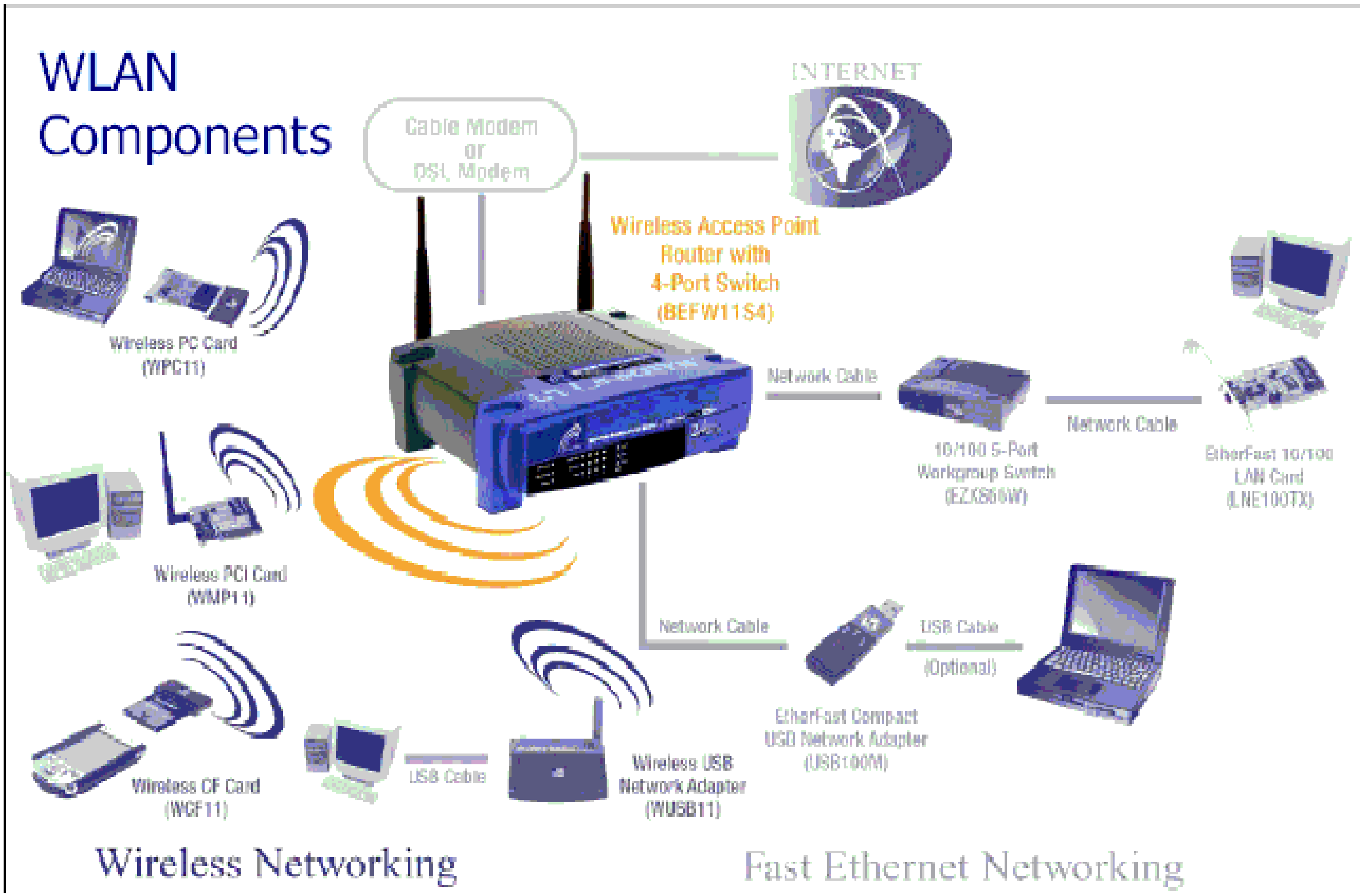
IEEE 802.11 Wireless Networks

- 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

  & 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

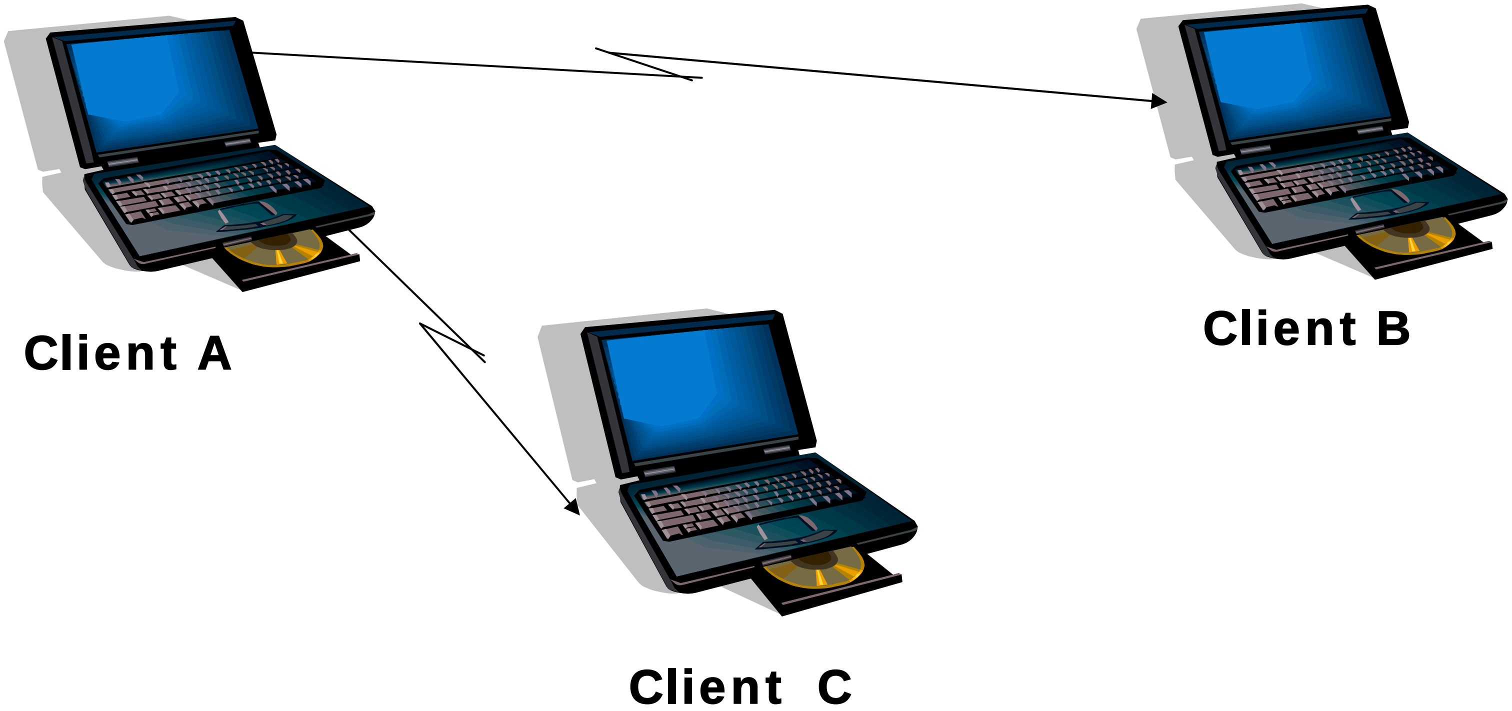


More about WLAN

Modes of Operation

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

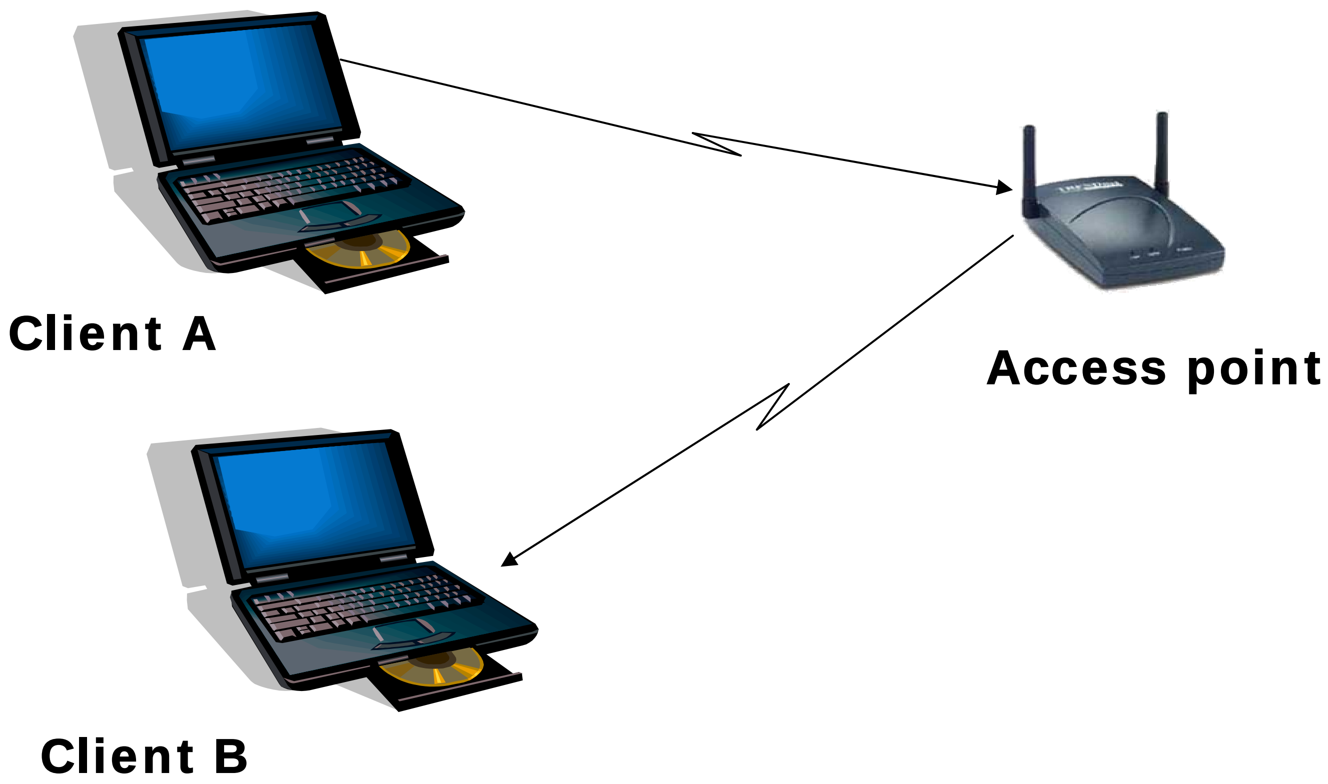
Ad-Hoc mode



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.

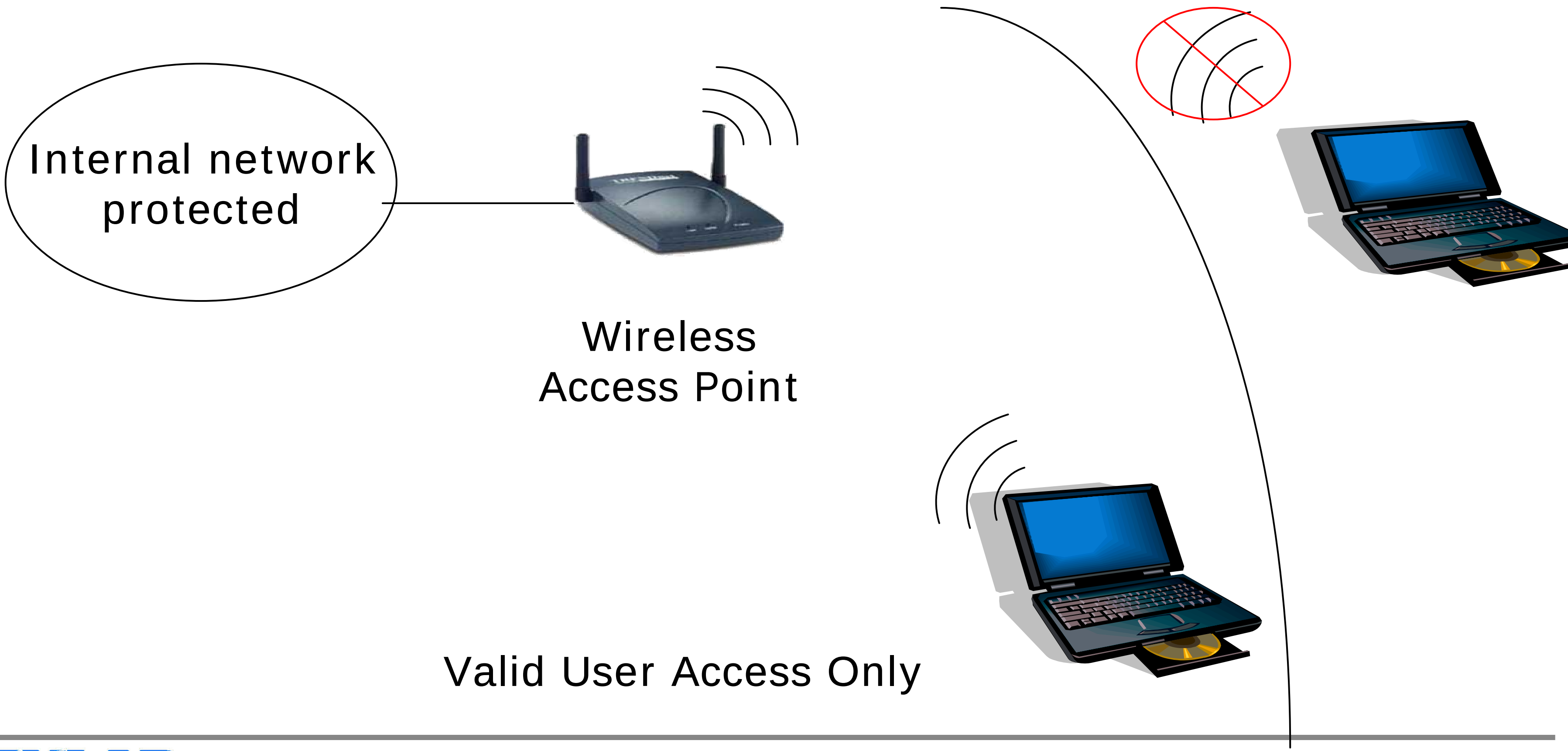
Infrastructure mode

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.



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.



IEEE 802.11 Basic Security Mechanisms

- Service Set Identifier (SSID)
- MAC Address filtering

- Wired Equivalent Privacy (WEP) protocol

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

Service Set Identifier (SSID) and their limits!

- 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 chooses an AP to associate with based upon its SSID.
- 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 a little stronger security than SSID

Disadvantages :

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

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).
- 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.

Nominal throughput (Mbps)	Actual throughput (bps)*		
	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

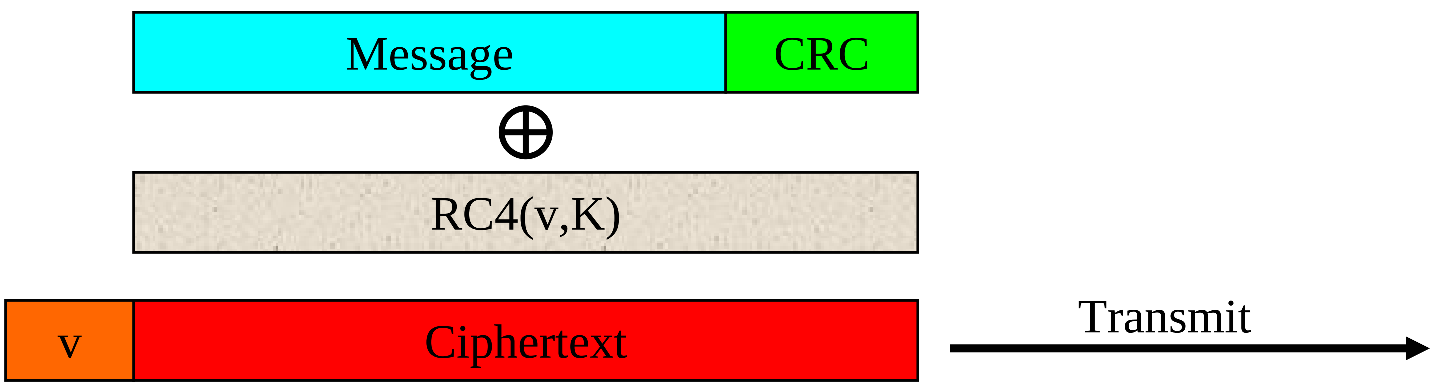
WEP Overview

- WEP relies on a shared key K between communicating parties

1. **Checksum:** For a message M, we calculate c(M). The plaintext is P={M,c(M)}
2. **Encryption:** The plaintext is encrypted using RC4. RC4 requires an initialization vector (IV) v, and the key K. Output is a stream of bits called the keystream. Encryption is XOR with P.

$$C = P \oplus RC4(v, K)$$

3. **Transmission:** The IV and the ciphertext C are transmitted.



WEP Security Goals

- WEP had three main security goals:
  - Confidentiality: Prevent eavesdropping
  - Access Control: Prevent inappropriate use of 802.11 network, such as facilitate dropping of not-authorized packets
  - Data Integrity: Ensure that messages are not altered or tampered with in transit
- The basic WEP standard uses a 40-bit key (with 24bit IV)
- Additionally, many implementations allow for 104-bit key (with 24bit IV)
- None of the three goals are provided in WEP due to serious security design flaws and the fact that it is easy to eavesdrop on WLAN

WEP (Vernam) Key Stream Reuse

- Vernam-style stream ciphers are susceptible to attacks when same IV and key are reused:

$$
\begin{aligned}
C_1 &= P_1 \oplus RC4(v, K) \\
C_2 &= P_2 \oplus RC4(v, K) \\
C_1 \oplus C_2 &= P_1 \oplus RC4(v, K) \oplus P_2 \oplus RC4(v, K) \\
&= P_1 \oplus P_2
\end{aligned}
$$

- Particularly weak to known plaintext attack: If P_1 is known, then P_2 is easy to find (as is RC4).
  – This might occur when contextual information gives P_1 (e.g. application-level or network-level information reveals information)
- Even so, there are techniques to recover P_1 and P_2 when just (P_1 XOR P_2) is known (frequency analysis, crib dragging)
  – Example, look for two texts that XOR to same value

WEP's Proposed Fix

- WEP's engineers were aware (it seems??) of this weakness and required a per-packet IV strategy to vary key stream generation
- Problems:
  - Keys, K, typically stay fixed and so eventual reuse of IV means eventual repetition of keystream!!
  - IVs are transmitted in the clear, so its trivial to detect IV reuse
  - Many cards set IV to 0 at startup and increment IV sequentially from there
  - Even so, the IV is only 24 bits!
- Calculation: Suppose you send 1500 byte packets at 5Mbps, then 2^{24} possible IVs will be used up in 11.2 hours!
- Even worse: we should expect to see atleast one collision after 5000 packets are sent!
- Thus, we will see the same IV again… and again…

WEP Decryption Dictionaries

- Once a plaintext is known for an IV collision, the adversary can obtain the key stream for **that specific** IV!
- The adversary can gather the keystream for each IV collision he observes
  - As he does so, it becomes progressively easier to decrypt future messages (and he will get improved context information!)
  - The adversary can build a dictionary of (IV, keystream)
- This dictionary attack is effective regardless of keysize as it only depends on IV size!

WEP Weakness in Message Authentication

- The checksum used by WEP is CRC-32, which is not a cryptographic checksum (MAC)
  - Purpose of checksum is to see if noise modified the message, not to prevent "malicious" and intelligent modifications
- Property of CRC: The checksum is a linear function of the message

$$c(x \oplus y) = c(x) \oplus c(y)$$

- This property allows one to make controlled modifications to a ciphertext without disrupting the checksum:
  - Suppose ciphertext C is: $$C = RC4(v, K) \oplus \{M, c(M)\}$$
  - We can make a new ciphertext C' that corresponds to an M' of our choosing
  - Then we can spoof the source by: A→B: {v,C'}

WEP: Spoofing the Source

- Our goal: Produce an M’=M+δ, and a corresponding checksum that will pass checksum test. (Hence, we will need to make a plaintext P’={M’,c(M’)} and a corresponding ciphertext C’)
- Start by choosing our own δ value, and calculate checksum.
- Observe:

$$
\begin{aligned}
C' &= C \oplus \{\delta, c(\delta)\} \\
&= RC4(v,K) \oplus \{M, c(M)\} \oplus \{\delta, c(\delta)\} \\
&= RC4(v,K) \oplus \{M \oplus \delta, c(M) \oplus c(\delta)\} \\
&= RC4(v,K) \oplus \{M', c(M \oplus \delta)\} \\
&= RC4(v,K) \oplus \{M', c(M')\}
\end{aligned}
$$

- Thus, we have produced a new plaintext of our choosing and made a corresponding ciphertext C’
- Does not require knowledge of M, actually, we can choose δ to flip bits!

WEP Message Injection (No Access Control!)

- Property: The WEP checksum is an unkeyed function of the message.
- If attacker can obtain an entire plaintext corresponding to a frame, he will then be able to inject arbitrary traffic into the network (for same IV):

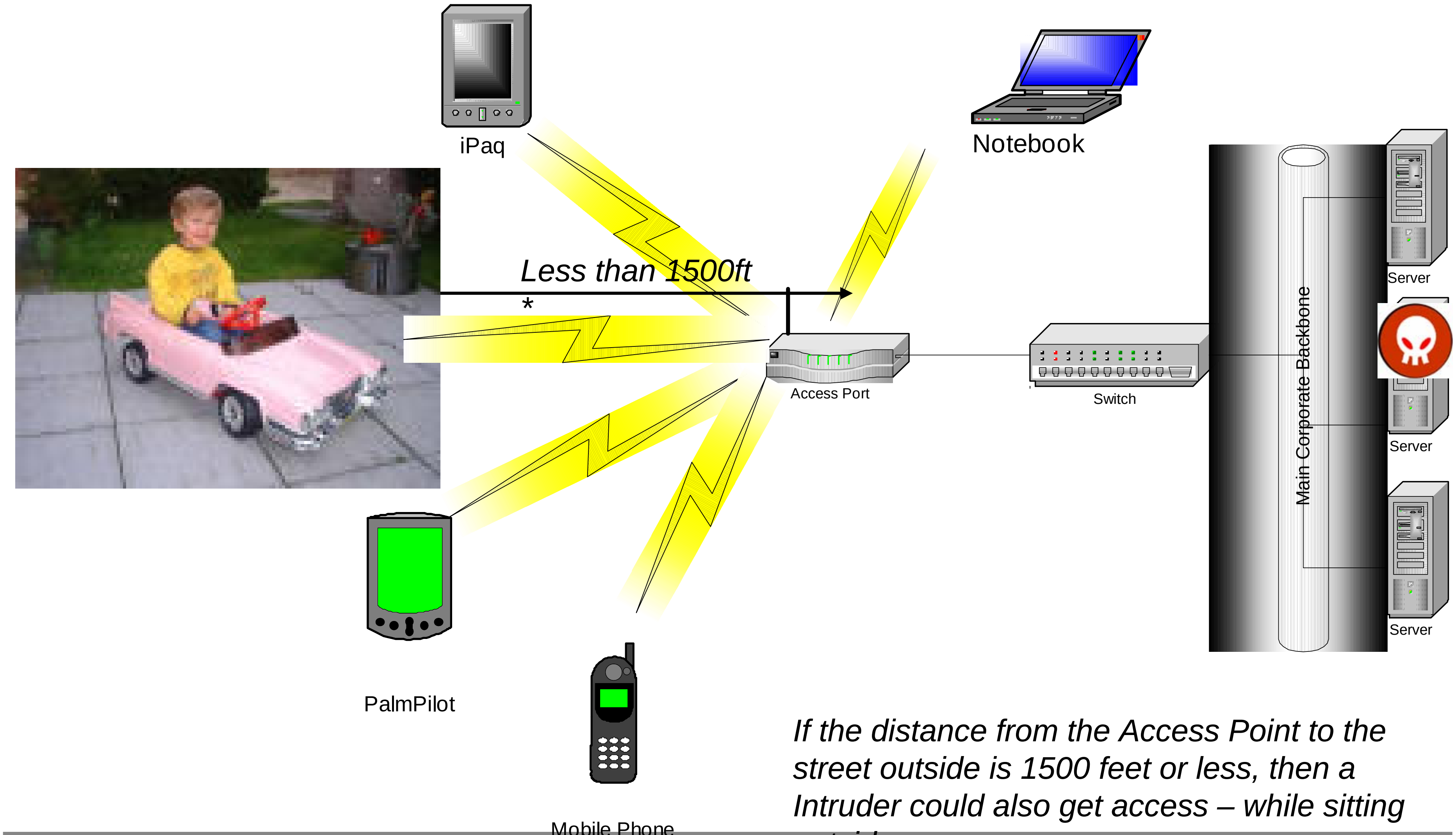
1. Get RC4(v,K)
2. For any message M' form $C' = RC4(v, K) \oplus \{M', c(M')\}$

- Why did this work? c(M) only depended on M and not on any key!!!
- (Note: An adversary can easily masquerade as an AP since there are no mechanisms to prevent IV reuse at the AP-level!)

Other Security Problems of 802.11

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

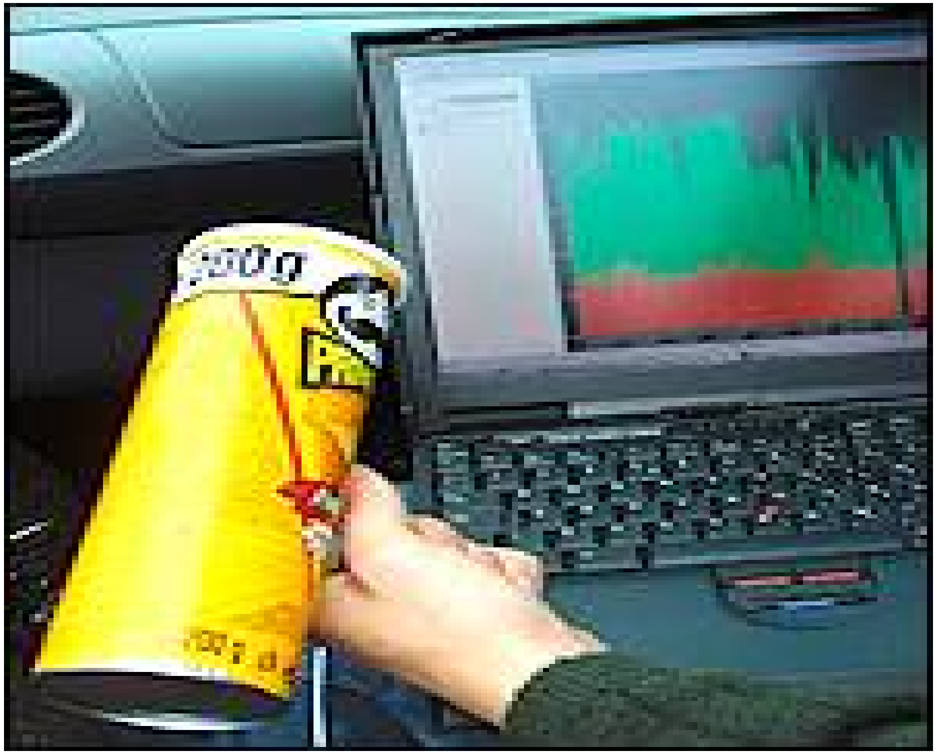
Drive By Hacking



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

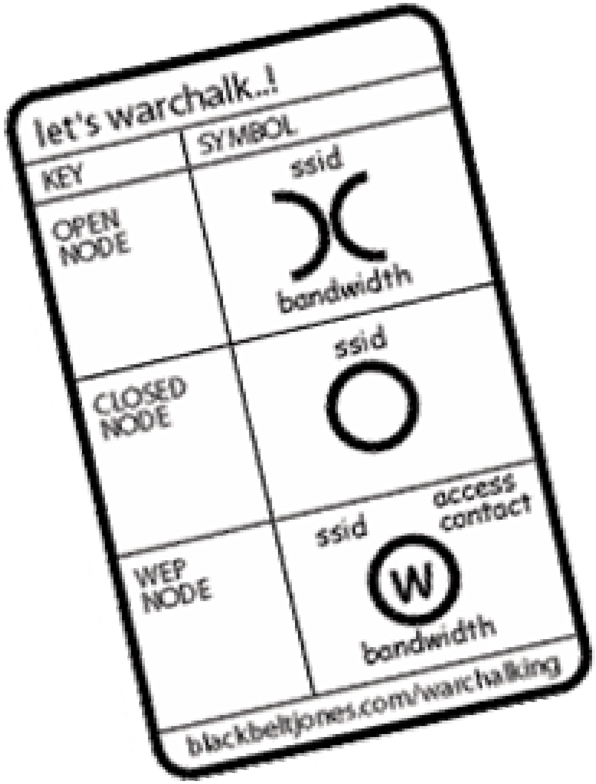
War-driving expeditions

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



War Chalking

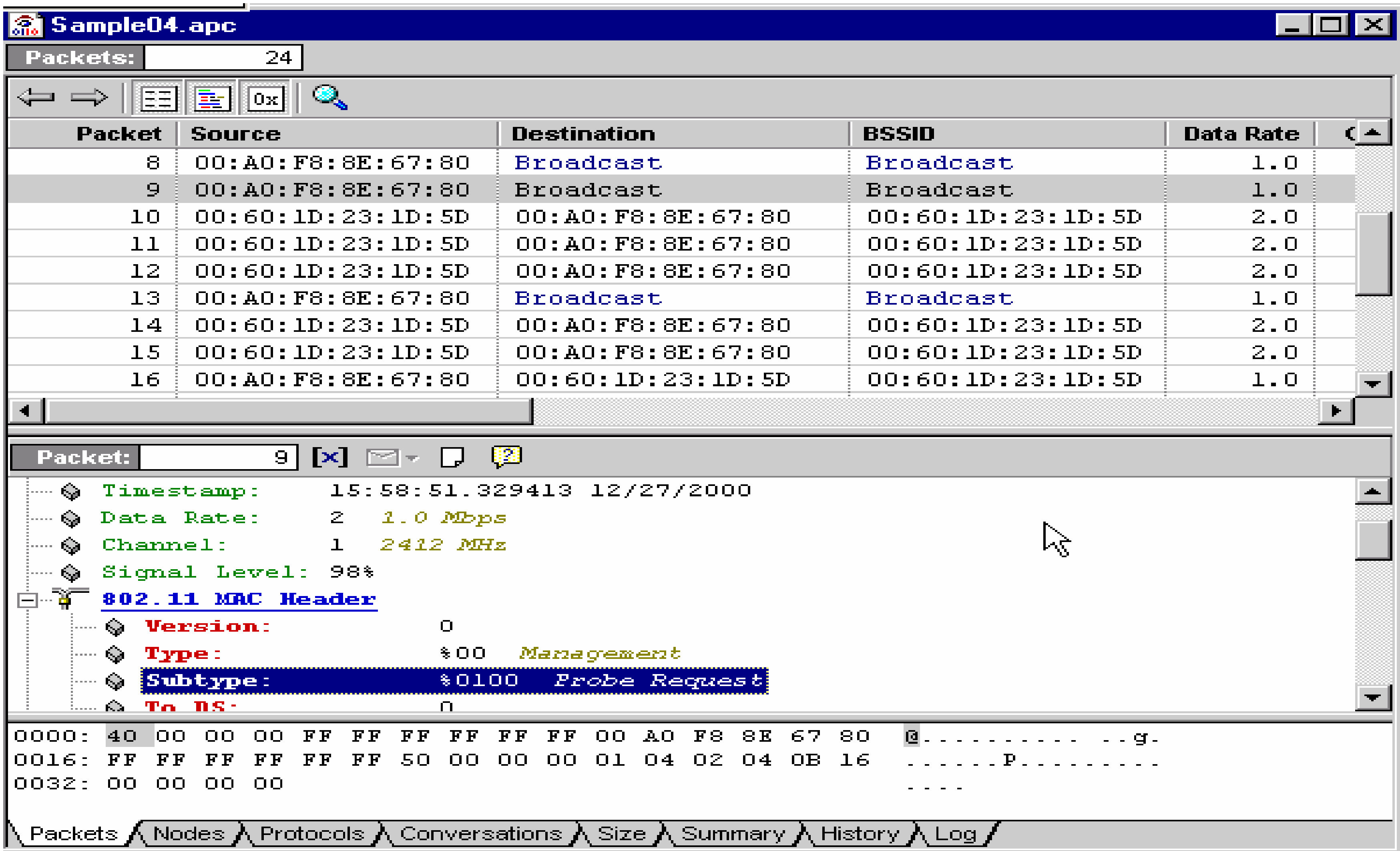
- Practice of marking a series of symbols on sidewalks and walls to indicate nearby wireless access. That way, other computer users can pop open their laptops and connect to the Internet wirelessly.



What are the major security risks to 802.11b?

- Insertion Attacks (Intrusions!)
- Interception and monitoring wireless traffic
- Misconfiguration
- Jamming
- Client to Client Attacks (Intrusions also!)

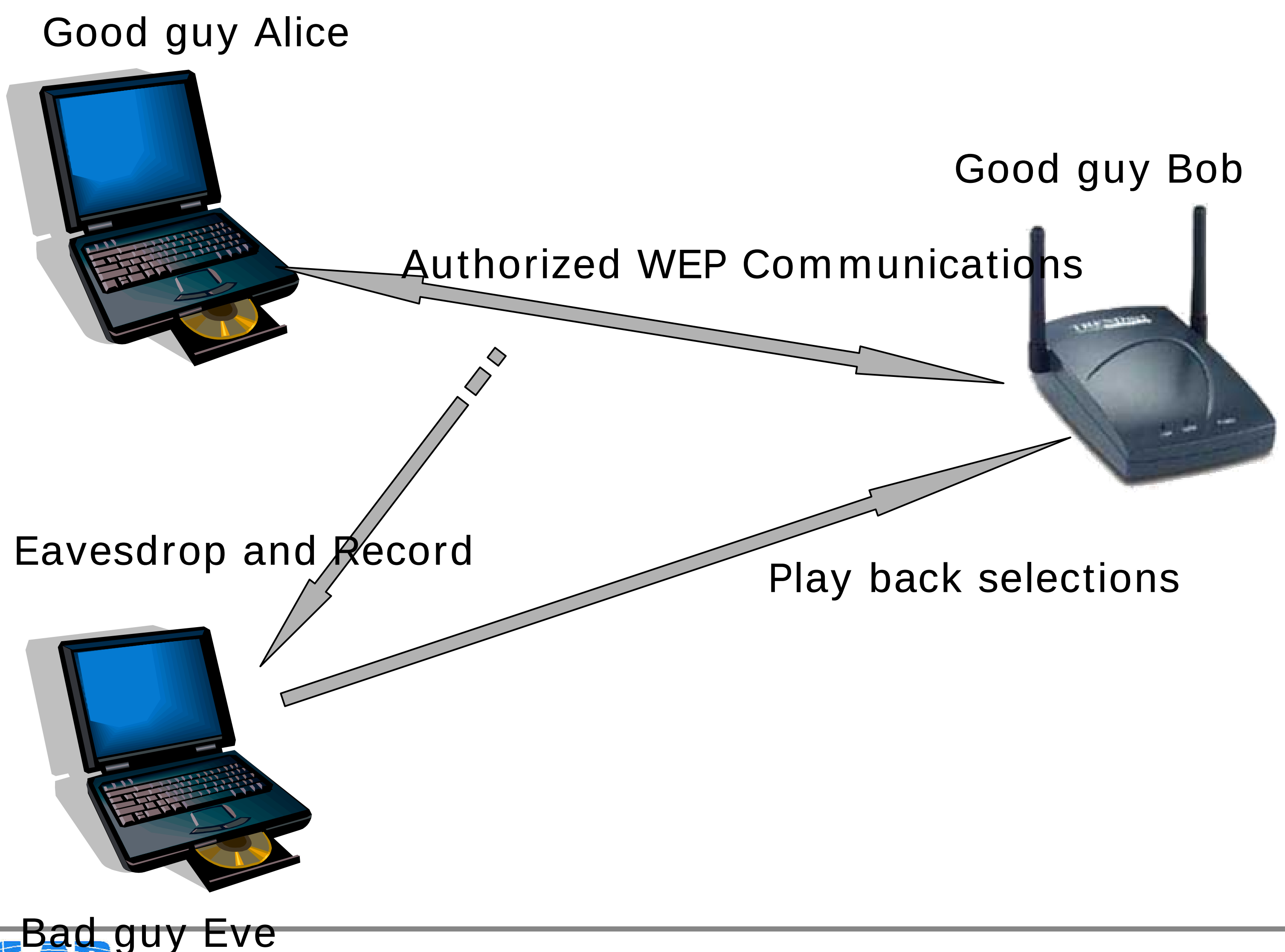
Packet Sniffing



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.
- Waveform Generators
- Microwave

Replay Attack



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
- Choose complex admin password
- Apply Filtering
- Use MAC (hardware) address to restrict access
- The Use of 802.1x
- Enable firewall function

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)
- 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)