



# Network II

## CS 184

Wireless (In)Security -- WEP

Department of Computer Science  
George Washington University

# Additional Resources

- Intercepting Mobile Communications: The Insecurity of 802.11 by Nikita Borisov, Ian Goldberg, and David Wagner.
  - Published in Seventh Annual International Conference on Mobile Computing and Networking, 2001.
- Wireless LAN Security: A Short History
  - <http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html>

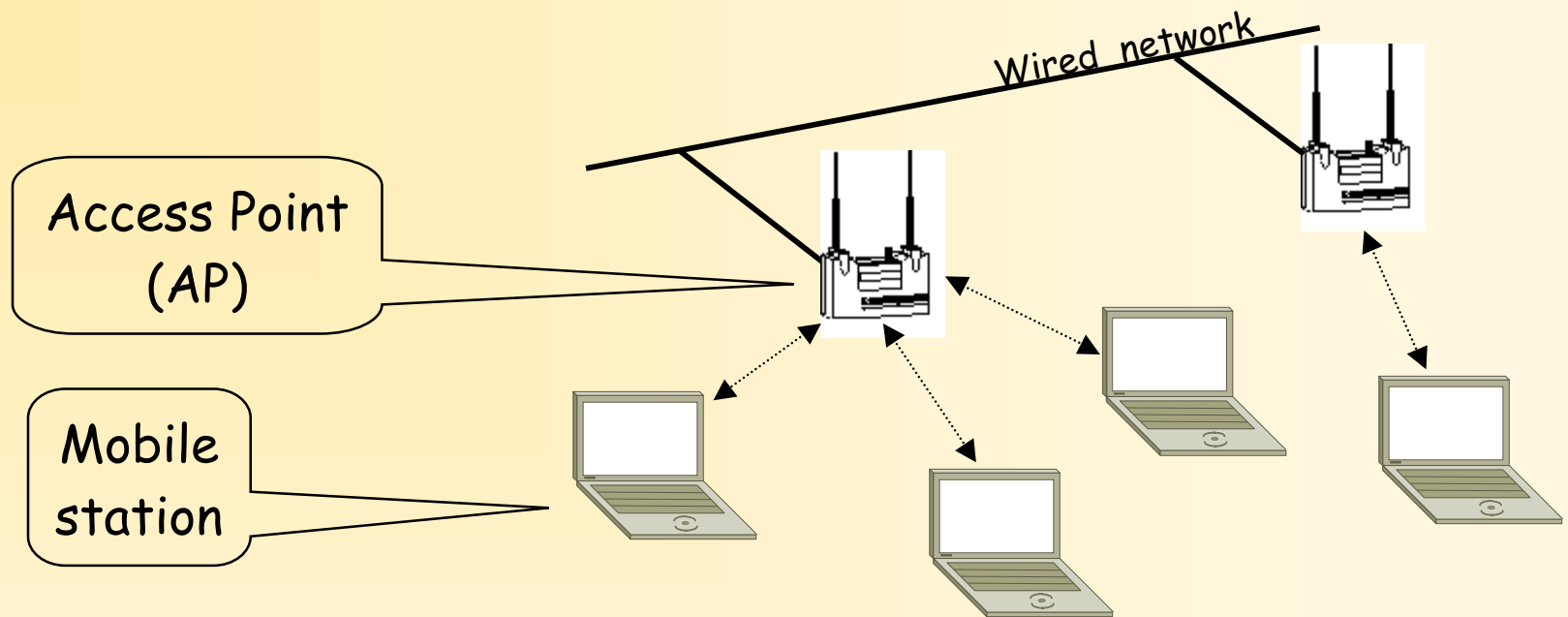
# 802.11 Wireless Security

- Wireless LAN networks are commonly built with the 802.11 protocol suite (802.11a,b,g,X)

Specifies standard networking functions over radio waves

- Transparent layer for upper network protocols (IP, TCP, Novell NetWare, ...)
  - Implements wireless networks (WLAN)
  - Integrates seamlessly into a LAN
  - Works on any platform, given drivers
- Fast: up to 11Mbit/s (802.11b) or 54Mbit/s (802.11a, g)
  - Ethernet is 10Mbit/s, fast Ethernet 100Mbit/s
  - Range about 30m/100feet
- Widely deployed
  - PCMCIA cards, built into Apple laptops, embedded solutions

# Infrastructure Mode



- Access points connect to wired network
- Multiple mobile stations per AP
  - Full internet connection for mobile users
    - University campus
    - Coffee shops
    - airport lounges, ...

# Data Transmission

For both LANs and WLANs

- Communication broken into *frames*
  - Variable length (up to ~ 1,500 byte)
- *Header* associated with frame
  - Source address
  - Destination address
  - Frame length, ...
- *Packet* = header + frame

# Subverting Communication

## WLAN

- Eavesdropping
  - Hardware widely sold
  - Proximity of source
    - Parking lot attack
- Injecting traffic
  - Just send to network
  - May need to modify driver setup
- Removing traffic
  - Scramble radio signal

## LAN

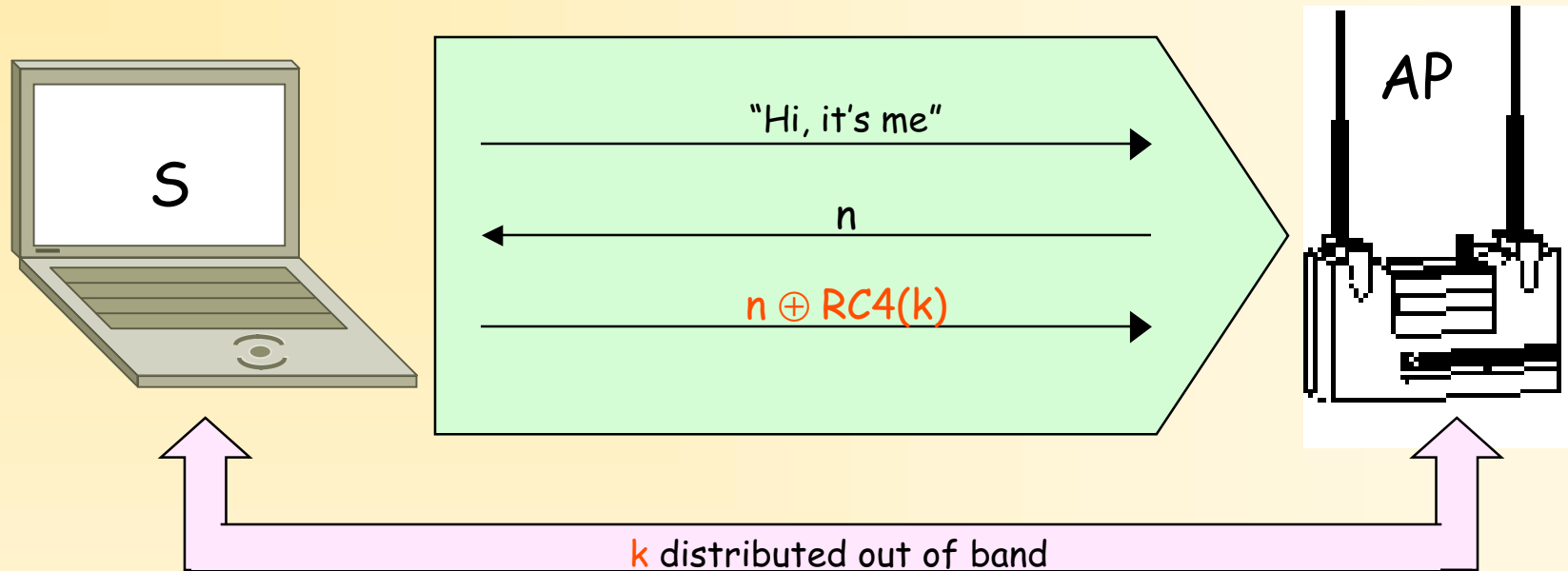
- Eavesdropping
  - Plug in laptop
  - Need access to wire
    - Hardly unnoticeable
- Injecting traffic
  - Just send to network
  - May need to modify driver setup
- Removing traffic
  - Feasible

# WEP - Wired Equivalent Privacy

Security mechanism for WLANs

- 2 subsystems
  - Station authentication
    - Simulate wired access control
  - Data encapsulation
    - Create privacy of wired network
- Part of 802.11 standard

# WEP Authentication



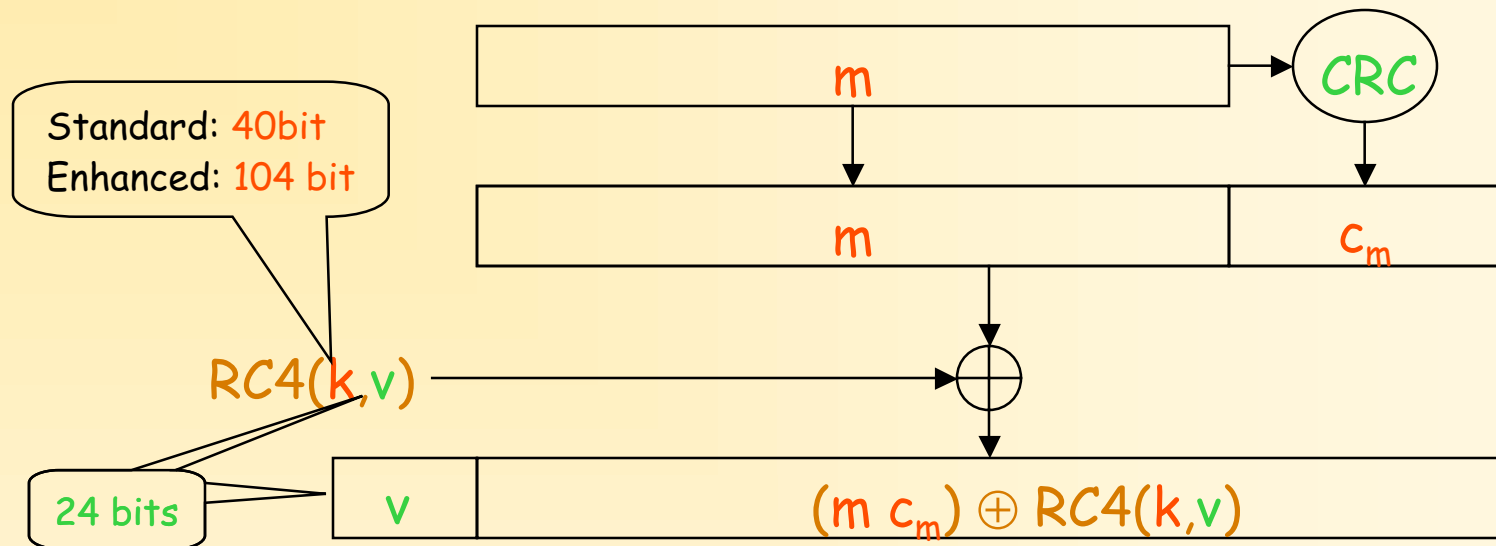
- S and AP share key  $k$ 
  - 802.11 standard: 40 bit
  - Most vendors now offer 104 bits (advertised as 128 bit!)
- $n$  is randomly generated nonce
- S is accepted only if last message decrypts to  $n$

# Data Encapsulation

A wants to send frame  $m$  to B

- Encapsulation (A)
  - Compute CRC-32 integrity checksum  $c_m$  of  $m$ 
    - Public algorithm, does not depend on  $k$
  - Compute keystream  $RC4(k,v)$ 
    - RC4 is secure keystream function (proprietary RSA)
    - $v$  is 24 bit initialization vector (IV)
  - Broadcast  $v, x = v, ((m \ c_m) \oplus RC4(k,v))$
- Decapsulation (B)
  - $x \oplus RC4(k,v) = m \ c_m$

# ... Pictorially



- Checksum guarantees data integrity
- IV
  - Prevents reuse of keystream
    - WEP does not prescribe modification of IVs
  - Sent with each packet

# WEP Security Goals

- Confidentiality
  - Prevent eavesdropping
- Access control
  - Prevent unauthorized access
- Integrity
  - Prevent tempering with messages

WEP does not achieve any of them!

# Keystream Reuse

## WEP collision

- If  $x_1 = ((m_1 \ c_{m_1}) \oplus \text{RC4}(k, v))$   
and  $x_2 = ((m_2 \ c_{m_2}) \oplus \text{RC4}(k, v))$
- Then  $x_1 \oplus x_2 = (m_1 \ c_{m_1}) \oplus (m_2 \ c_{m_2})$

- Independent from key length!
- Recognizing collisions
  - $k$  changes very seldom, if ever
  - Generally, all stations use same  $k$
  - $v$  sent in clear with every packet
- Look for packets with the same IV

# Likelihood of Keystream Reuse

Given  $r_1, \dots, r_n \in [0, 1, \dots, B]$   
If  $n \geq 1.2\sqrt{B}$ ,  
then  $\text{Prob}[\exists i \neq j : r_i = r_j] > 0.5$

- Ideal case
  - By birthday paradox
    - 50% chances of collision after ~5000 packets
    - < 4 minutes at 5Mbit/s (packets of 1500 bytes)
- In practice, IVs are poorly generated
  - Many PCMCIA cards
    - IV=0 when inserted
    - incremented by 1 at each packet
  - Few thousand IVs determine most traffic
- 802.11 does not require changing IV

# Attacks

$$\begin{array}{l} \text{If } x_1 = ((m_1 \ c_{m_1}) \oplus \text{RC4}(k,v)) \\ \text{and } x_2 = ((m_2 \ c_{m_2}) \oplus \text{RC4}(k,v)) \\ \text{then } x_1 \oplus x_2 = (m_1 \ c_{m_1}) \oplus (m_2 \ c_{m_2}) \end{array}$$

- Passive attacks
  - Exploit message redundancy
    - Many fields of IP header are predictable
    - Login sequences (e.g. Password: )
    - Transfer of shared libraries, ...
- Active attacks
  - Send spam to mobile host
  - Have mobile host send you email, ...
- Dumb attacks
  - Some APs send frames unencrypted also

# Decryption Dictionaries

- Once packet is revealed, keystream is known
- Build table of intercepted keystreams
  - Maps every  $v$  to  $RC4(k, v)$
  - Requires  $\sim 24\text{Gb}$  for  $2^{24}$  for 1,500 byte frames
  - Less than 1Gb with PCMCIA IV generation
- Then, one can decrypt all traffic

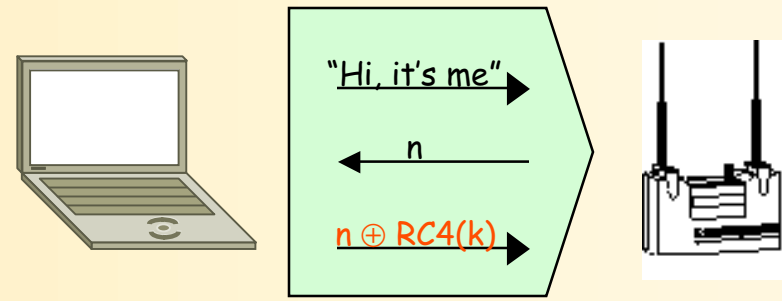
# Key Management

- 802.11 does not specify how to
  - Generate
  - Distribute
  - Update shared key (and how often)
- In practice
  - Key is loaded in device by hand when set up
    - Often keep manufacturer's default
  - Never updated again
  - Attacker has years to compromise key
    - A few hours are enough for 40 bit version

# Restoring Confidentiality

- IV is too short
  - Collisions frequency reduced with longer IVs
  - Relatively small decryption dictionary
- IV update unspecified (and non required)
  - Force collision resistant IV generation
  - From keyed random number generator
- Key management inexistent
  - Introduce mandatory key update protocol
  - Force different key for each host

# Gaining Access



Trivial !

- Record one authentication exchange
  - from  $(n, n \oplus RC4(k))$ , recover  $RC4(k)$
  - Use it to encrypt all future authentication challenges
- Remedy
  - Use different cipher for authentication
    - A block cipher would do

# Analysis of a Débacle

Why is WEP so bad??

- International standard
- Backed by big vendors (IBM, 3COM, Apple, ...)
- Written by communication engineers
  - “Keep packet length small”
  - “Be conservative in what you send, liberal in what you accept”
  - Not security people involved
  - Opaque design (no public review before standardization)
  - Could have profited from IPSec experience
- Should operate with limited resource
  - Cell phones, PDAs, ...

# The Future of WEP

## Proposal for a new standard 802.1X

- Use stream cipher based on AES
- Sequence number to avoid replays
- Replace CRC with MAC
- Authentication based on Kerberos

# Information Slide

- Ethereal assignment (exercise1) due on Thursday in printed form.
- Lecture slides can be obtained at the course web page  
<http://www.seas.gwu.edu/~jonathan/courses/cs184>