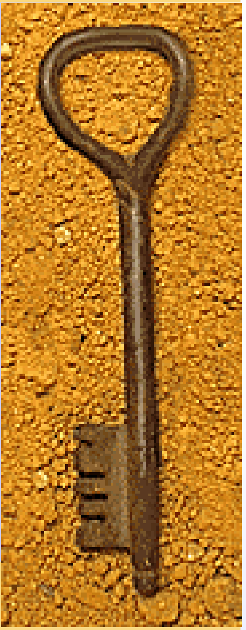
Graduate Course on **Computer Security**

Lecture 6: Case Study II - WEP

Iliano Cervesato iliano@itd.nrl.navy.mil

ITT Industries, Inc @ NRL - Washington DC

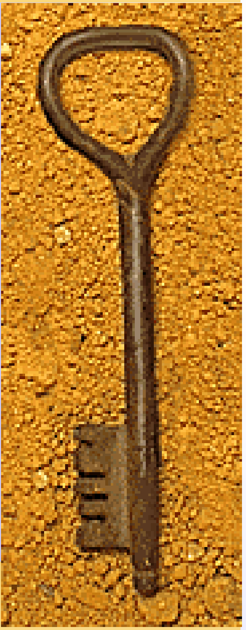
http://www.cs.stanford.edu/~iliano/



Outline

- The 802.11 wireless communication standard
- WEP: Wired Equivalent Privacy
  - Architecture
  - Security goals
  - Attacks
    - Confidentiality
    - Authentication
    - Integrity
  - Lessons Learned

The IEEE 802.11 Standard

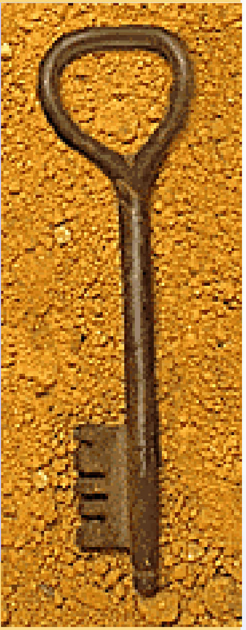


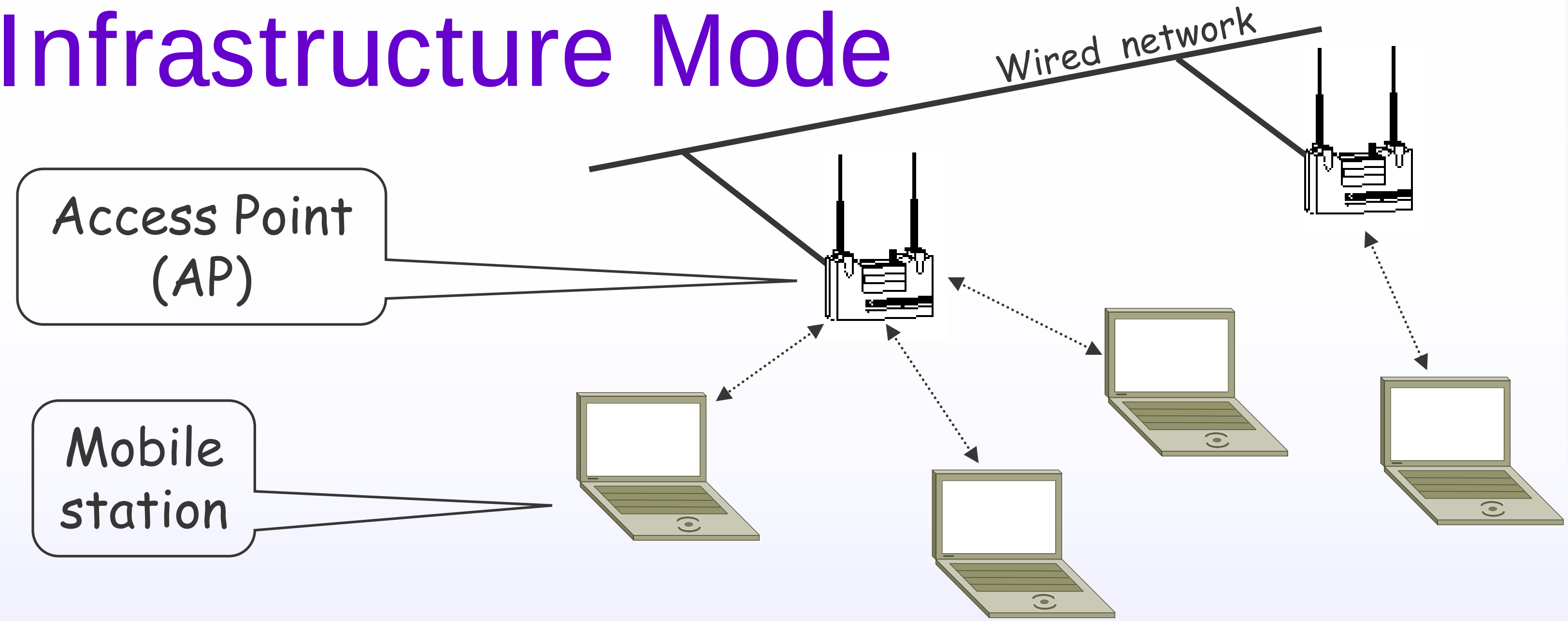
802.11
WEP
Secrecy
Access
Integrity
Lessons

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
  - Ethernet is 10Mbit/s, fast Ethernet 100Mbit/s
  - Range about 30m/100feet
- Widely deployed
  - PCMCIA cards, ISA bus cards, embedded solutions, …
  - Offered by major vendors

Infrastructure Mode

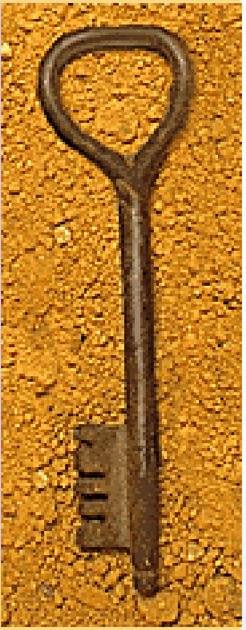


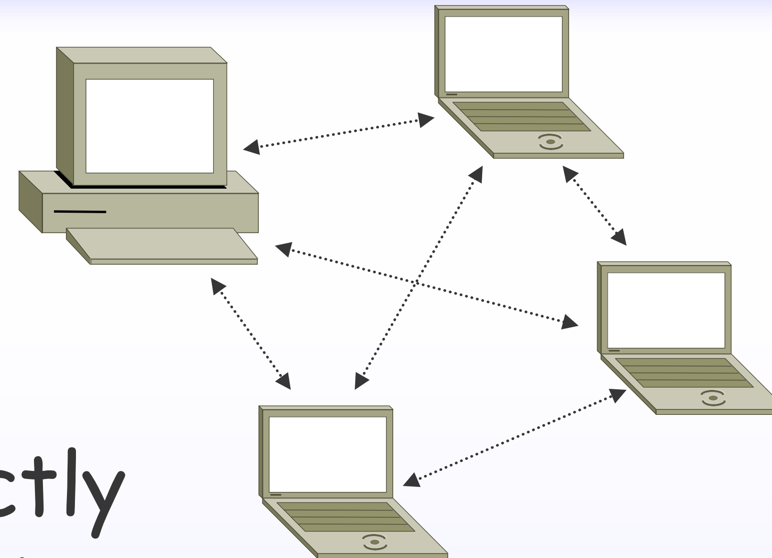


802.11
WEP
Secrecy
Access
Integrity
Lessons

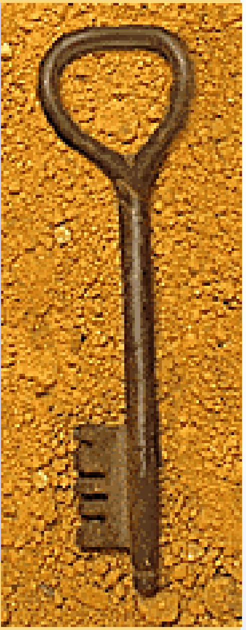
- Access points connect to wired network
- Multiple mobile stations per AP
  - Full internet connection for mobile users
    - University campus
    - Coffee shops
    - airport lounges, …

Ad Hoc Mode





- Wireless stations communicate directly
  - Communication without a wired network
    - On the fly networking
      - Impromptu meeting
    - LAN set up is difficult
      - Monitoring volcanoes
      - Study of jungle canopy
    - LAN set up is dangerous
      - War zones

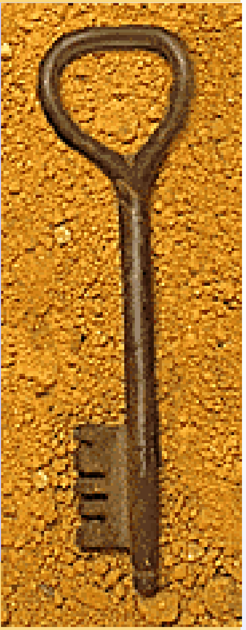


Data Transmission

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



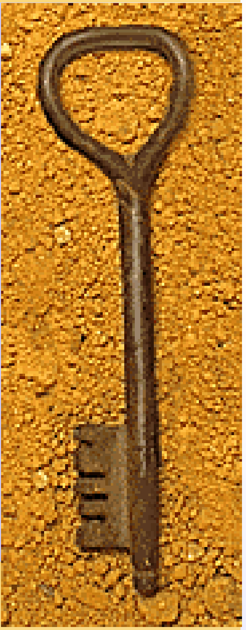
WLAN

- 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

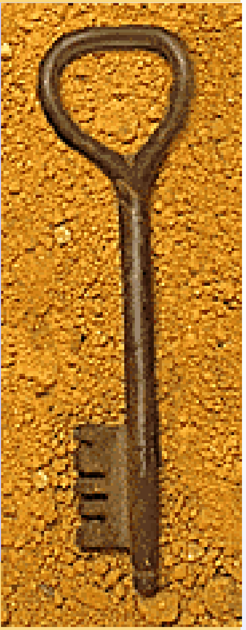
WEP – Wired Equivalent Privacy



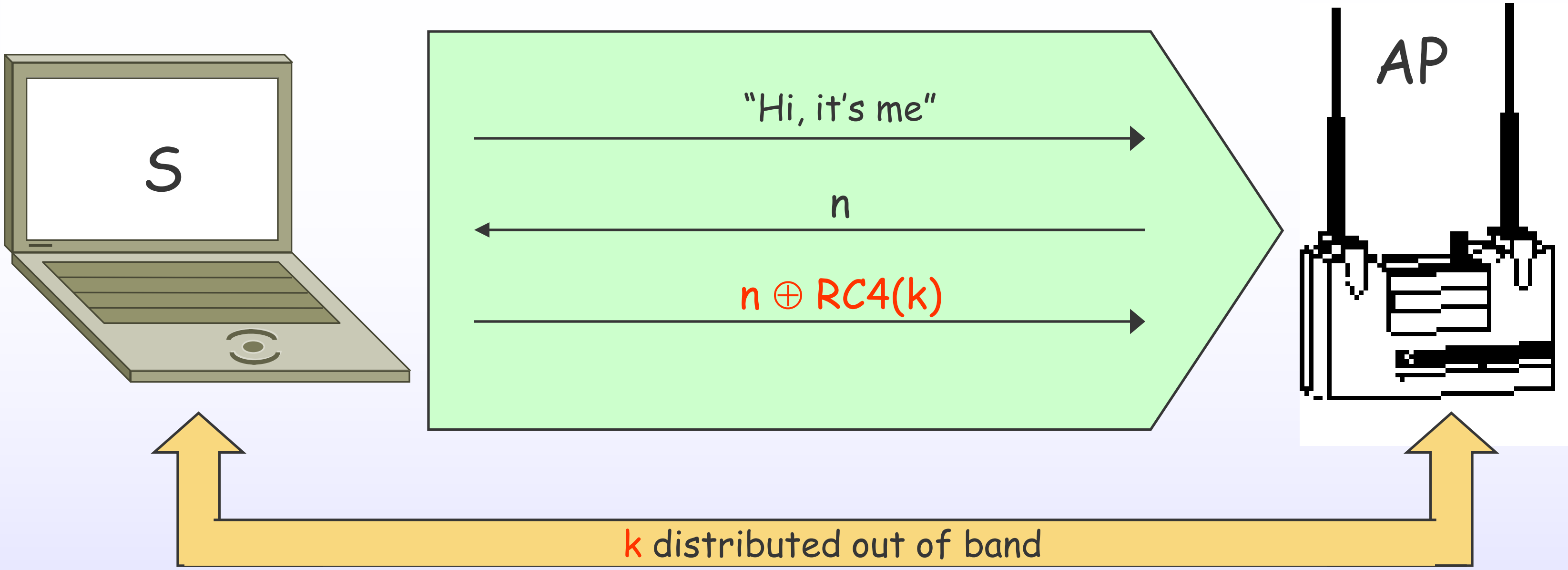
802.11
WEP
Secrecy
Access
Integrity
Lessons

Security mechanism for WLANs

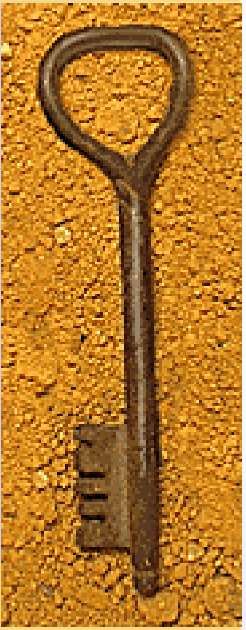
- 2 subsystems
  - Station authentication
    - Simulate wired access control
  - Data encapsulation
    - Create privacy of wired network
- Part of 802.11 standard



WEP Authentication



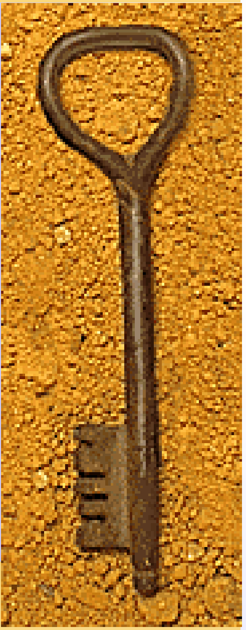
- S and AP share key k
  - 802.11 standard: 40 bit
  - Most vendors now offer 104 bits (advertised as 128 bit!)
- n is randomly generated nonce
- S is accepted only if last message decrypts to n



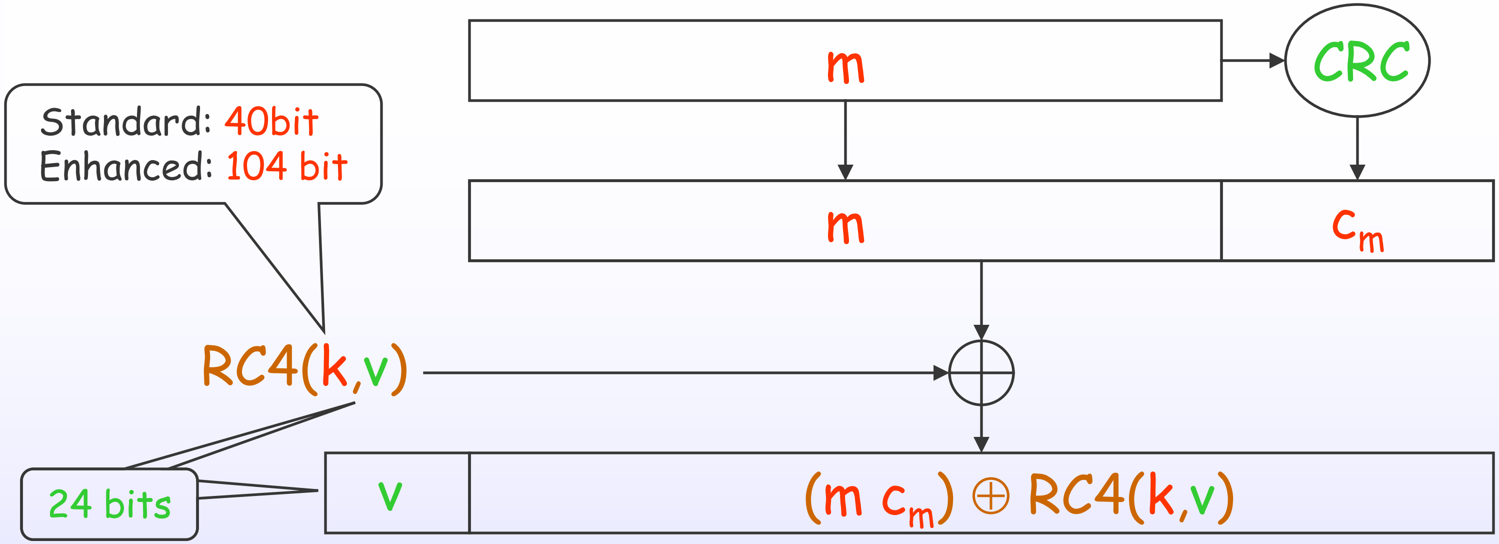
Data Encapsulation

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)
  - $x \oplus RC4(k,v)) = m\ c_m$

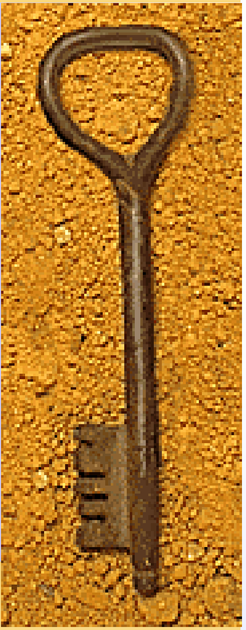


… Pictorially



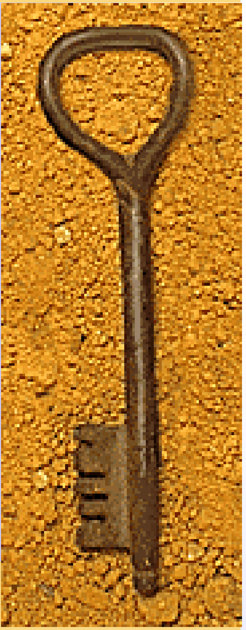
- Checksum guarantees data integrity
- IV
  - Prevents reuse of keystream
    - WEP does not prescribe modification of IVs
  - Sent with each packet

WEP Security Goals



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

WEP does not achieve any of them!



802.11
WEP
Secrecy
Access
Integrity
Lessons

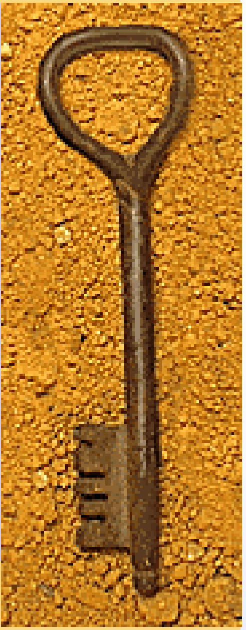
Keystream Reuse

WEP collision

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

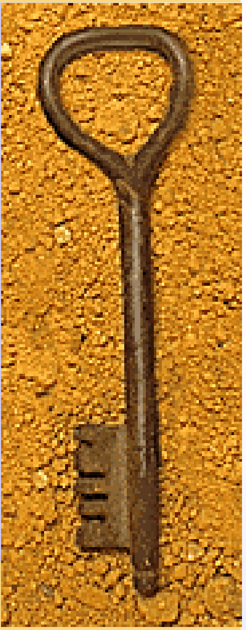


802.11
WEP
Secrecy
Access
Integrity
Lessons

Likelihood of Keystream Reuse

Given $r_1, \ldots r_n \in [0, 1, \ldots, B]$
If $n \geq 1.2\sqrt{B}$,
then $\text{Prob}[\exists\, i \neq j : r_i = r_j] > \frac{1}{2}$

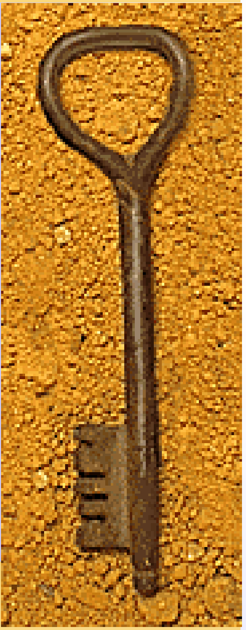
- Ideal case
  - By birthday paradox
    - 50% chances of collision after ~5000 packets
    - < 4 minutes at 5Mbit/s (packets of 1500 bytes)
    - All 2^{24} keystreams recovered in $\frac{1}{2}$ day
- In practice, IVs are poorly generated
  - Many PCMCIA cards
    - IV=0 when inserted
    - incremented by 1 at each packet
  - Few thousand IVs determine most traffic
- 802.11 does not require changing IV



Attacks

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

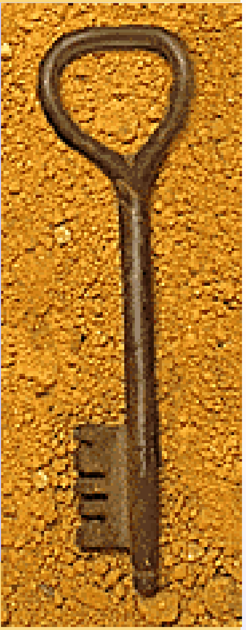
- Passive attacks
  - Exploit message redundancy
    - Many fields of IP header are predictable
    - Login sequences (e.g. `Password:`)
    - Transfer of shared libraries, …
- Active attacks
  - Send spam to mobile host
  - Have mobile host send you email, …
- Dumb attacks
  - Some APs send frames unencrypted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



Decryption Dictionaries

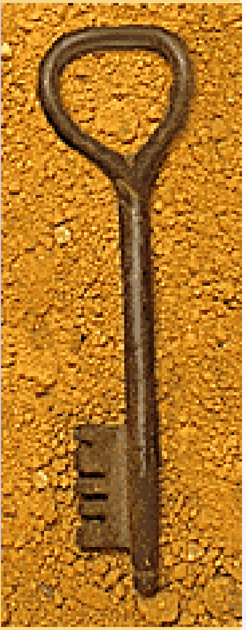
- Once packet is revealed, keystream is known
- Build table of intercepted keystreams
  - Maps every v to RC4(k,v))
  - Requires ~24Gb for 2^{24} for 1,500 byte frames
  - Less than 1Gb with PCMCIA IV generation
- Then, can decrypt all traffic

Key Management



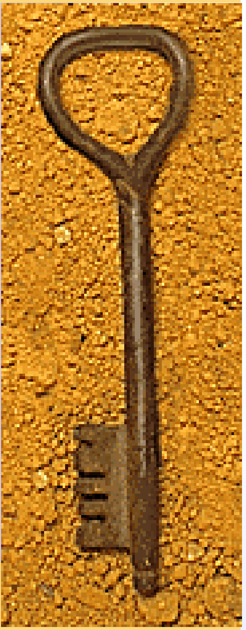
- 802.11 does not specify how to
  - Generate
  - Distribute
  - Update shared key (and how often)
- In practice
  - Key is loaded in device by hand when set up
    - Often keep manufacturer's default
  - Never updated again
  - Attacker has years to compromise key
    - A few hours are enough for 40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

Restoring Confidentiality

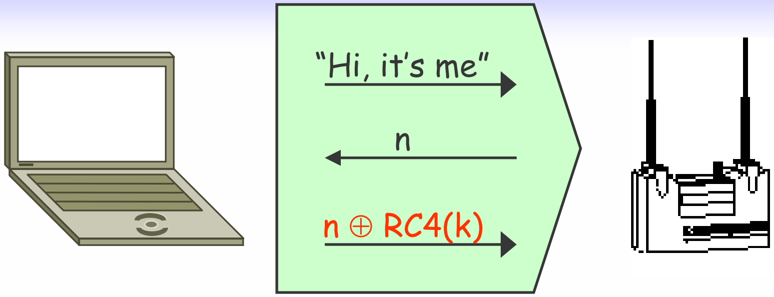


802.11
WEP
Secrecy
Access
Integrity
Lessons

- 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

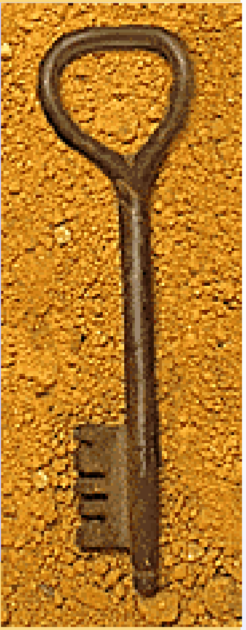


Gaining Access



Trivial !

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



Perturbing Traffic

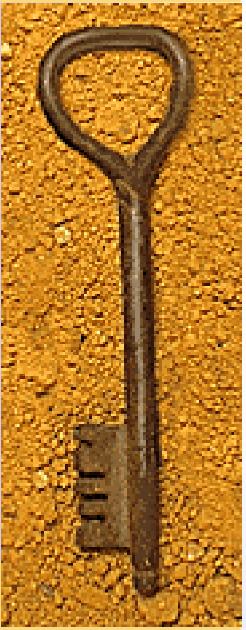
Integrity protected by CRC-32 checksum

- Checksums are linear w.r.t. $\oplus$

$$c_{m \oplus m'} = c_m \oplus c_{m'}$$

- Then for any Δ, xor'ing any ciphertext x with (Δ c_Δ) will go undetected

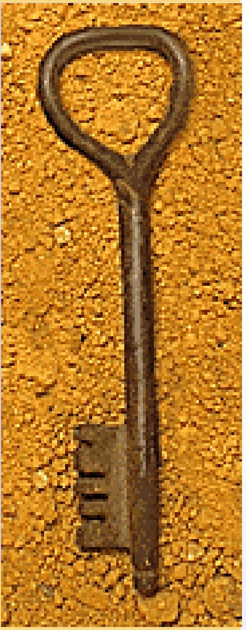
- Remedy
  - … exercise



Targeted Traffic Alteration

- Linearity of CRC limited to flipping bits
- Use format of frames to force bit values
  - E.g. IP header
- Build decryption dictionary

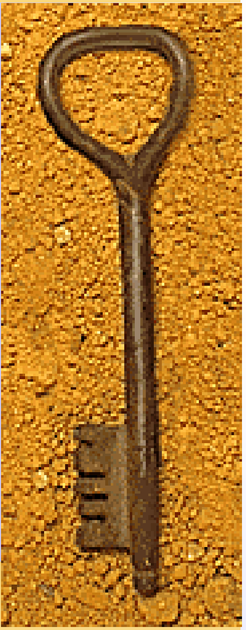
Analysis of a Débacle



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, …

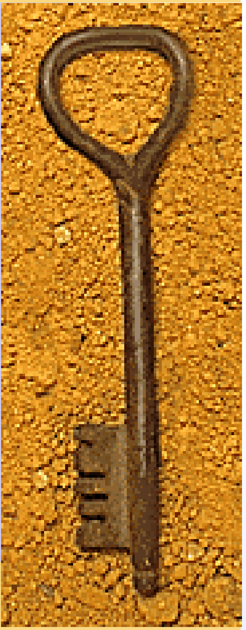


802.11
WEP
Secrecy
Access
Integrity
Lessons

The Future of WEP

Proposal for a new standard 802.1X

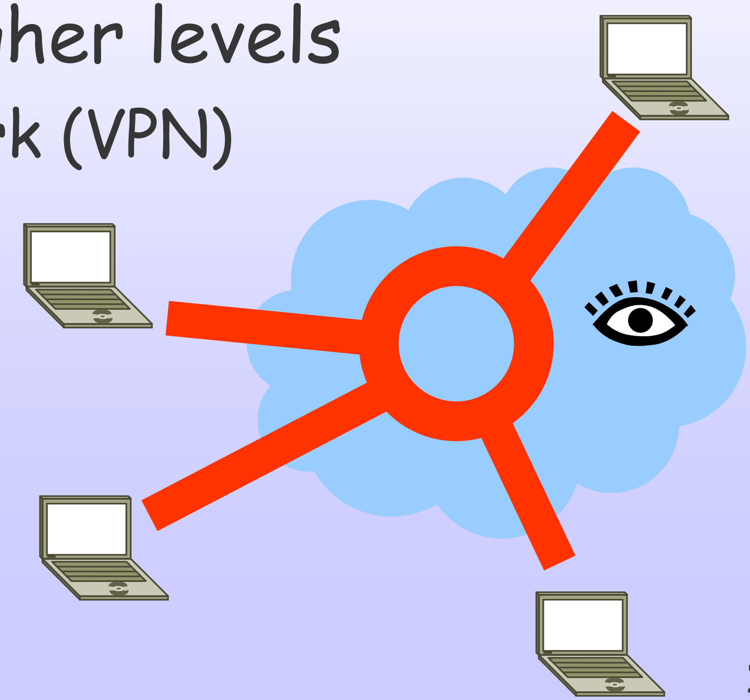
- Use stream cipher based on AES
- Sequence number to avoid replays
- Replace CRC with MAC
- Authentication based on Kerberos



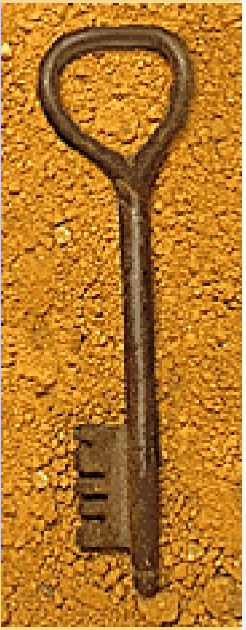
Should You Go Wireless?

YES!

- 802.11 is a fine communication suite
- Handle security at higher levels
  - Virtual Private Network (VPN)
  - IPSec
  - … or just what you normally use!



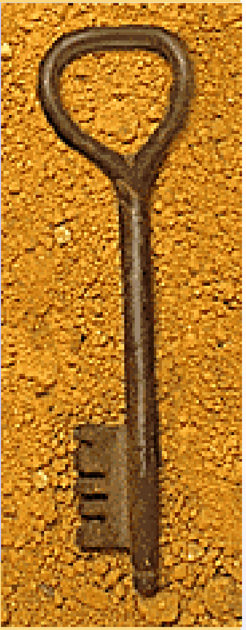
Readings



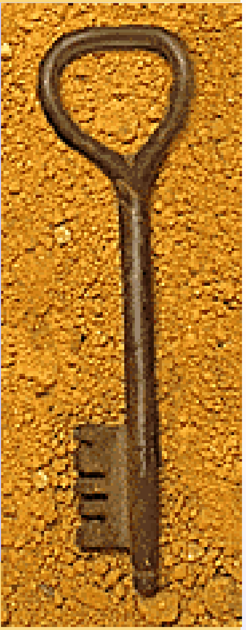
802.11
WEP
Secrecy
Access
Integrity
Lessons

- N. Borisov, I. Goldberg and D. Wagner, *Intercepting Mobile Communications: the Insecurity of 802.11*, 2001
- W. Arbaugh, N. Shankar, and Y. Wan, *Your 802.11 Wireless Network has no Clothes*, 2001
- IEEE 802.11 Working Group web page, `http://grouper.ieee.org/groups/802/11`
- Jesse Walker, "Overview of 802.11 Security", 2001

Exercises for Lecture 6



- Prove that
  - if $x = ((m\ c_m) \oplus RC4(k,v))$,
  - Then $x \oplus (\Delta\ c_\Delta)$ has a correct checksum for every Δ
- Suggest a remedy for traffic perturbation



802.11
WEP
Secrecy
Access
Integrity
Lessons

Next ...

- Specification Languages