Wireless LAN Security

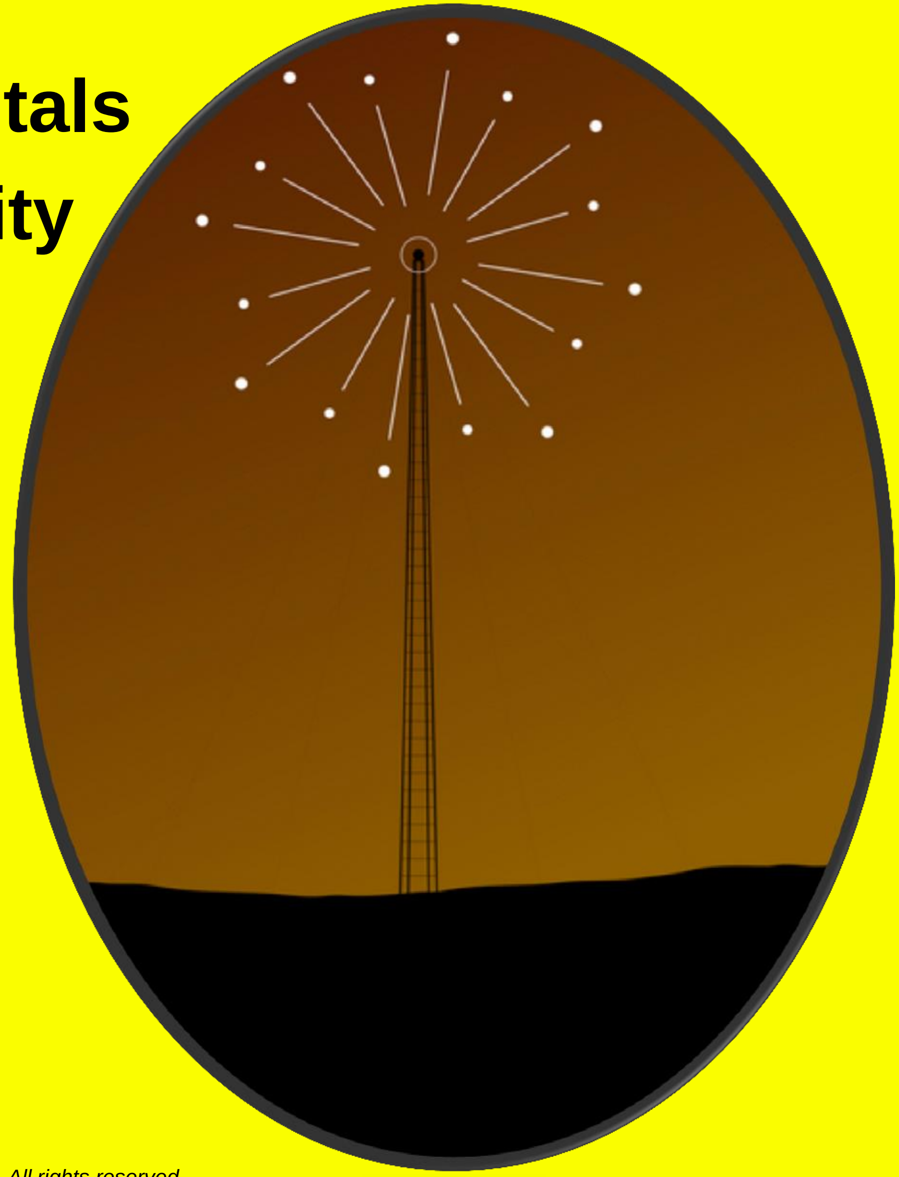
This slide set includes information not in the textbook chapter.

CSH6 Chapter 33
"Wireless LAN Security"

Gary L. Tagg & Jason Sinchak

Topics

- Introduction
- 802.11 Security Fundamentals
- IEEE 802.11 Robust Security Network
- Fundamental Wireless Threats
- Specific Wireless Security Attacks
- Mitigating Controls
- Secure Enterprise Design
- Secure Auditing Tools



Introduction

- Scope
- Corporate Use of Wireless LANs
- Functional Benefits of Wireless
- Security Benefits of Wireless
- Centralized Management
- Overview & History of IEEE 802.11 Standards

Scope

- Massive adoption of IEEE 802.11 wireless LANs
- Mobility, flexibility, rapid deployment, costs
- New opportunities for unauthorized access
- Purpose of chapter
  - Introduce wireless technologies
  - Present issues
  - Offer ways of addressing issues
  - Open-source and commercial tools for auditing wireless networks

Corporate Uses of Wireless LANs

- Offices, plants, schools
  - Employee access throughout area (campus, warehouse…)
  - Meeting rooms
  - Access for external consultants, visitors
  - Work outside normal desk area (e.g., café)
  - Managers can show employees laptop display
  - Reduce voice telecom costs using VoWLANs
- Public hot spots
  - Hotels, coffee shops, airports….
    - ✓ Increased mobile work
- Rapid deployment: no cabling (esp. in older buildings or historical sites), avoid underground cabling

Functional Benefits

- Mobility; e.g.,
  - Warehouses
  - Shop floors
  - Hospitals
- Flexibility
  - Public hotspots widespread
  - Access outside corporate property
  - Access for visitors to corporate buildings
- Cost reductions
  - Reduce physical network infrastructure
  - Overloads handled automatically by shifting to nearby access points (APs)
  - Virtual LANs (VLANs) can use Service Set Identifiers (SSID) more easily than wired physical LANs

Security Benefits

- Physical security
  - Hide and shield APs
  - Contrast with physical network jacks – must be visible to all
- Segmentation visibility
  - Wired networks usually use Media Access Control (MAC) addresses
    - ✓ Define VLANs (virtual LANs) for specific areas or groups
    - ✓ Can be spoofed
    - ✓ Limit users to specific physical area
  - But wireless networks can assign per-SSID VLANs
    - ✓ Accessible anywhere in wireless environment

Centralized Management

- Wireless controllers can configure groups of APs
- Configure a single image for thin-client Aps
- User directory through Extensible Authentication Protocol–Remote Authentication Dial In User Service (EAP-RADIUS)
- Mesh of APs can support security monitoring
  - Wireless intrusion-detection systems (IDS)

Overview & History of IEEE 802.11 Standards

- History
  - Early 1990s – limited use of commercial protocols
  - Late 1990s – adoption of ANSI/IEEE 802.11 standard
    - ✓Baselines for interoperable products
  - 1999: 802.11b (11 Mbps)
  - 802.11a (54 Mbps) & 802.11g ↑ wireless bandwidth to = wired Ethernet LANs
  - 802.11n (2009)
    - ✓600 Mbps bandwidth
    - ✓Compatible with 802.11b
    - ✓5 GHz band

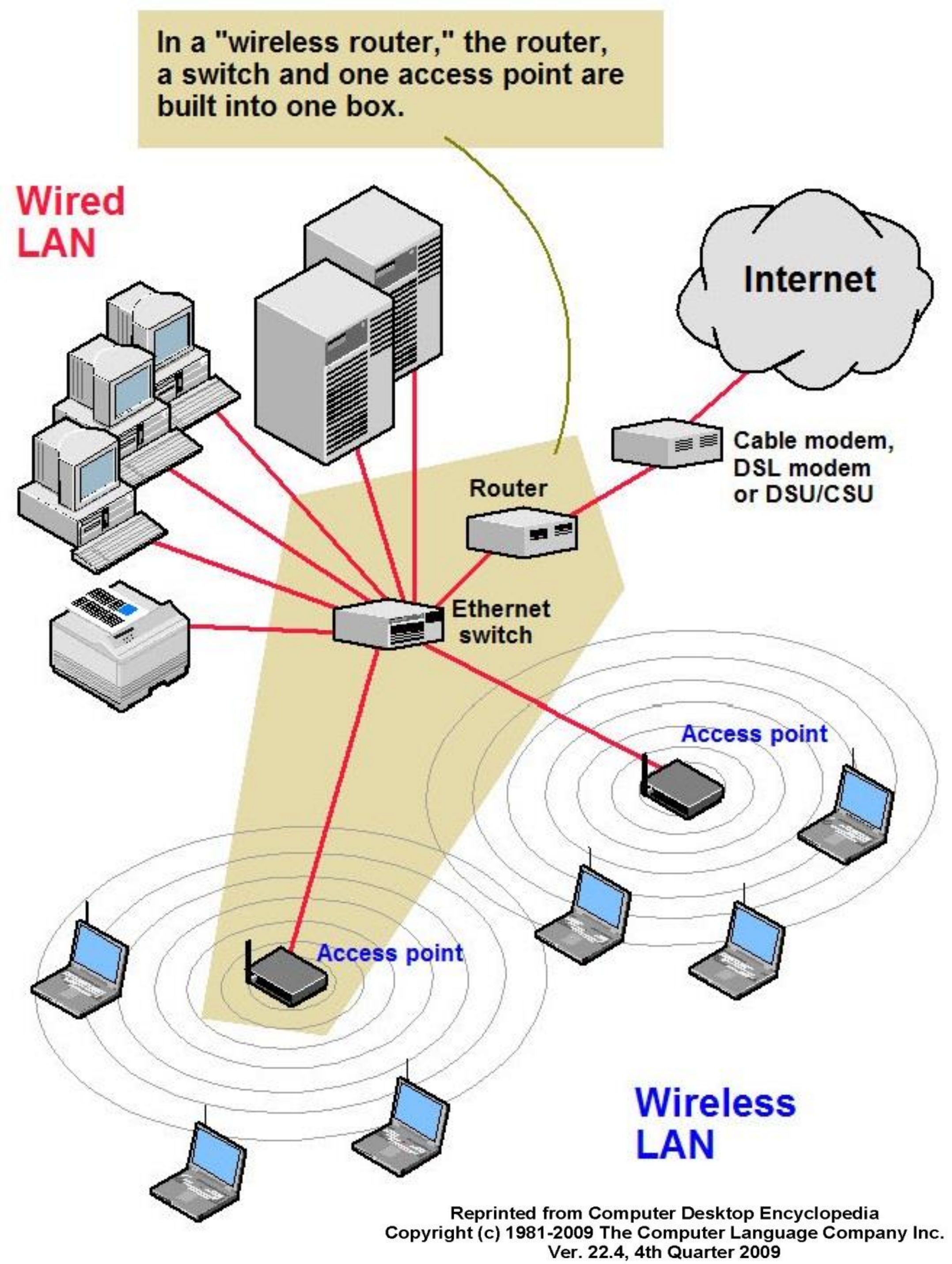
Home Use of Wireless LANs

- Wireless LAN networking grew explosively in 2000s
- Many homes use >1 computer
- Broadband Internet encourages telecommuting
- Computers can be away from telephone points
  - ❑Avoid running cables
- Wireless equipment no longer expensive

Architecture & Product Types

- 802.11 Components
- 802.11 Network Architecture
- 802.11 Physical Layer
- Wireless LAN Product Types
- Benefits of Wireless Switch/Access Controller Architecture
- Security Benefits of Wireless Switch/Access Controller Architecture

See RFC 4118 "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)"
http://www.faqs.org/ftp/rfc/pdf/rfc4118.txt.pdf

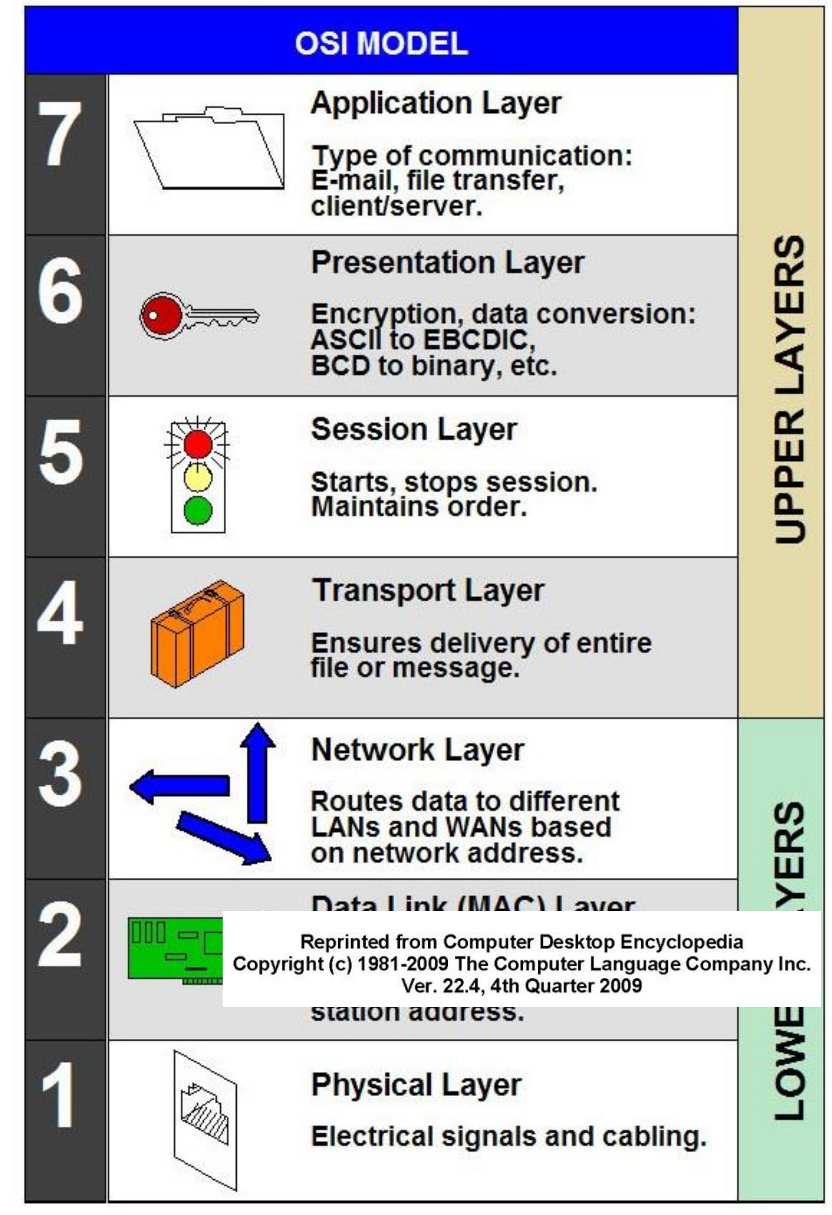


802.11 Components

- Stations (Sta)
- Access points (AP)
- Basic service sets (BSS)
  - 1 or more Sta linked to single AP
- Independent BSS (IBSS)
  - Ad hoc NW
  - Point to point (mesh)
- Extended service set (ESS)
  - Interconnected BSS + LANs = 1 BSS to Sta
- Distribution system (DS) & portal
  - Connect APs to form ESS
  - Portal: connects wired LAN with 802.11 NW

802.11 Network Architecture

- OSI ISO reference model
  - 802.11 provides services at physical & data link layers
- 802.11 layers
  - Physical (radio)
  - Medium Access Control
  - Logical Link Control



802.11 Physical Layer

- 802.11 Infrared (2 Mbps)
- 802.11 FHSS (Frequency-hopping spread spectrum)
    - 2 Mbps radio link in 2.4 GHz band
    - Defines 79 channels (1 MHz each)
- 802.11 DSSS (Direct sequence spread spectrum)
    - Also 2 Mbps radio link in 2.4 GHz
    - Spreads data over 14 channels (5 MHz each)
    - Increases bandwidth but limits channels to 3 in practice
- 802.11b DSSS (11 Mbps)
- 802.11 OFDM (Orthogonal frequency division multiplexing) – 54 Mbps in 5 GHz band
- 802.11g – OFDM in 2.4 GHz band for 54 Mbps
- 802.11n – 600 Mbps (IEEE working group)
    - 4 streams @ 40 MHz
    - Still under development (2009)

Wireless LAN Product Types (1)

- AP contains all functionality ("Fat" APs)
  - SOHO (small office/home office) users
  - Managing multiple fat APs became complex
- LWAP (lightweight AP)
  - Also use wireless switches in NW
  - Vendors developed different protocols
  - IETF working group: Control & Provisioning of Wireless Access Points (CAPWAP)
    - ✓RFC3390 – problem definition
    - ✓RFC4118 – taxonomy
    - ✓Developed CAPWAP protocol for interoperability

Wireless LAN Product Types (2)

- **Wireless Mesh Networks**
  - **Fat & LWAPs physically connected to wired NW (Internet access, LAN)**
  - **But wireless mesh design has point-to-point connections among APs**
  - **Much reduces cabling & deployment costs**
  - **IEEE established 802.11s working group**

Benefits of Wireless Switch / Access Controller Architecture

- Ease of deployment & management
- RF management
- Load-balancing users
- Simplified guest networking
- Fast roaming
- Layer 3 roaming (single IP address throughout campus)
- QOS (quality of service)
- Unification of wired & wireless
- AAA (authentication, authorization, accounting)
- Integration with older non-wired equivalent privacy (WPA/WPA2) equipment

Security Benefits of Wireless Switch / Access Controller Architecture

- User & device authentication
  - Only authorized users allowed
- Access control
  - Can assign user to specific VLAN
  - Handles guest access easily
- Inbuilt wireless intrusion detection & prevention
  - Can analyze every packet
- Rogue AP detection
  - Scan for unauthorized APs
  - Triangulate signals received at several APs
  - Some products can actively remove rogue APs

Wireless LAN Security Threats

General taxonomy of threats to networks

- Eavesdropping
- Masquerading (spoofing)
- Message modification*
- Replaying
- Denial of service
- Exploiting flaws in design, implementation or operation
- Cracking

* (MITM attacks)

Comparison Between Wired & Wireless

- Wireless NWs subject to long-distance penetration
  - High-gain aerials
  - Modified household satellite TV antennas
  - Cheap commercial products
- Corporate wired NWs generally protected
  - Firewalls
  - VPNs
- Wireless NWs much less secure
  - Easy to access by unauthorized people in street, parking area (or hill 20 miles away)
  - War-driving = roaming to find unprotected WAPs
- Operational management
  - Wired NWs usually run for professional IT personnel
  - Wireless NWs often installed by amateurs
  - Risk when WAPs attached to wireless NWs without authorization

Specific Threats Enabled by Wireless LANs

- Early 802.11 standards have security that has been completely broken
- 802.11i standard enhanced security BUT
  - New equipment includes compatibility with older standards
  - New security functionality generally not enabled by default
- Key security issues in “broken” 802.11 standards summarized on next slides

"How many days until we tell him that we don't need 'receptors' for the wireless?"

802.11 Security Issues

- Wireless NWs available outside physically controlled areas (use radio waves)
- NWs broadcast their existence
- Devices – not users – are authenticated (so stolen equipment usable)
- Original protocols easily broken
- Authentication is 1-way (client does not authenticate AP – allows rogue APs)
- WEP compromised
- Message integrity check vector (ICV) easily defeated using simple bit-flipping attacks
- Messages can be replayed without detection
- Admins install wireless LANs using default settings
- Wireless LANs use same keys for all users (so users can eavesdrop on each other)
- Public hot spots reveal confidential data

Specific Threats

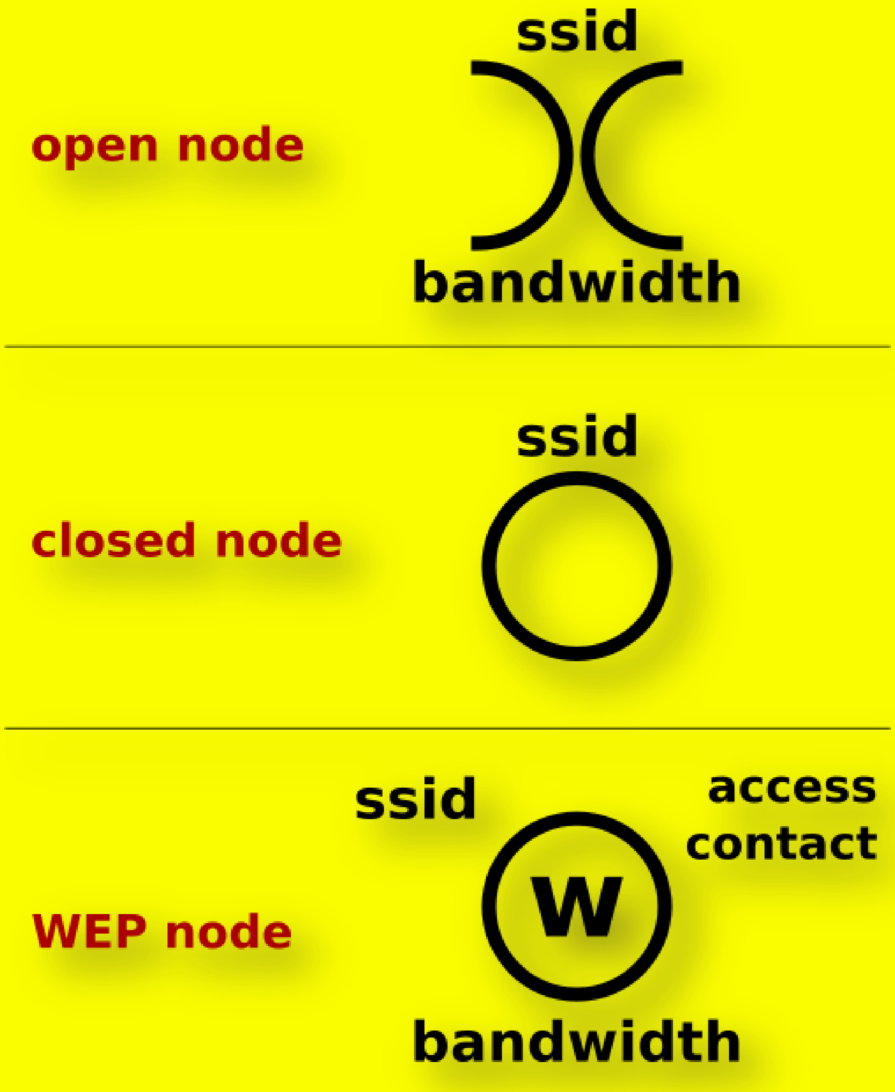
- War-Driving
- War-Chalking
- Dealing with War Drivers
- Laptops with 802.11
- Neighbors
- Hot Spots

War-Driving

- Peter Shipley (2000)
- Drive/walk around with wireless NW equipment
  - Laptop or handheld computer (smart phone)
  - Wireless access card & sw
- Results of early studies
  - >60% wireless NWs: default configuration
  - 15% used WEP
  - Most WLANs linked directly to corporate backbone
    - ✓Should have been to DMZ
    - ✓So 85% of WLANs gave unauthorized access to core NWs

War-Chalking

- Criminal hackers were marking pavement or wall showing availability of unprotect WAPs
- Activity has pretty much died out
- So easy to locate networks using, say, smart phone



Used without requiring permission – material defined as in public domain.
http://upload.wikimedia.org/wikipedia/commons/e/e6/Warchalking.svg

Dealing with War Drivers

- Video surveillance
- Brief physical/facilities security staff on recognizing war drivers
  - Stationary
  - Working on laptop
  - Pedestrians obvious; in car not so obvious
- Keep track of cars parked near building
- But in cities, war drivers can sit in coffee shops!
- MUST secure networks properly

Laptops & Phones with 802.11 (1)

- **Even low-end laptops have wireless capability**
- **Smart phones equipped**
- **Windows XP/7 WLAN client monitors for networks**
  - **May connect automatically**
  - **Significant problem for employees connecting to corporate networks from home, t**
  - **Rogue APs can take advantage of automatic connection**
- **Wireless units send out probes with identification of home network**
  - **So attacker can configure rogue AP**
  - **E.g., Linux-based HostAP**
  - **Once connected to laptop, attacker can scan for unprotected files, VPN tunnels to home system**

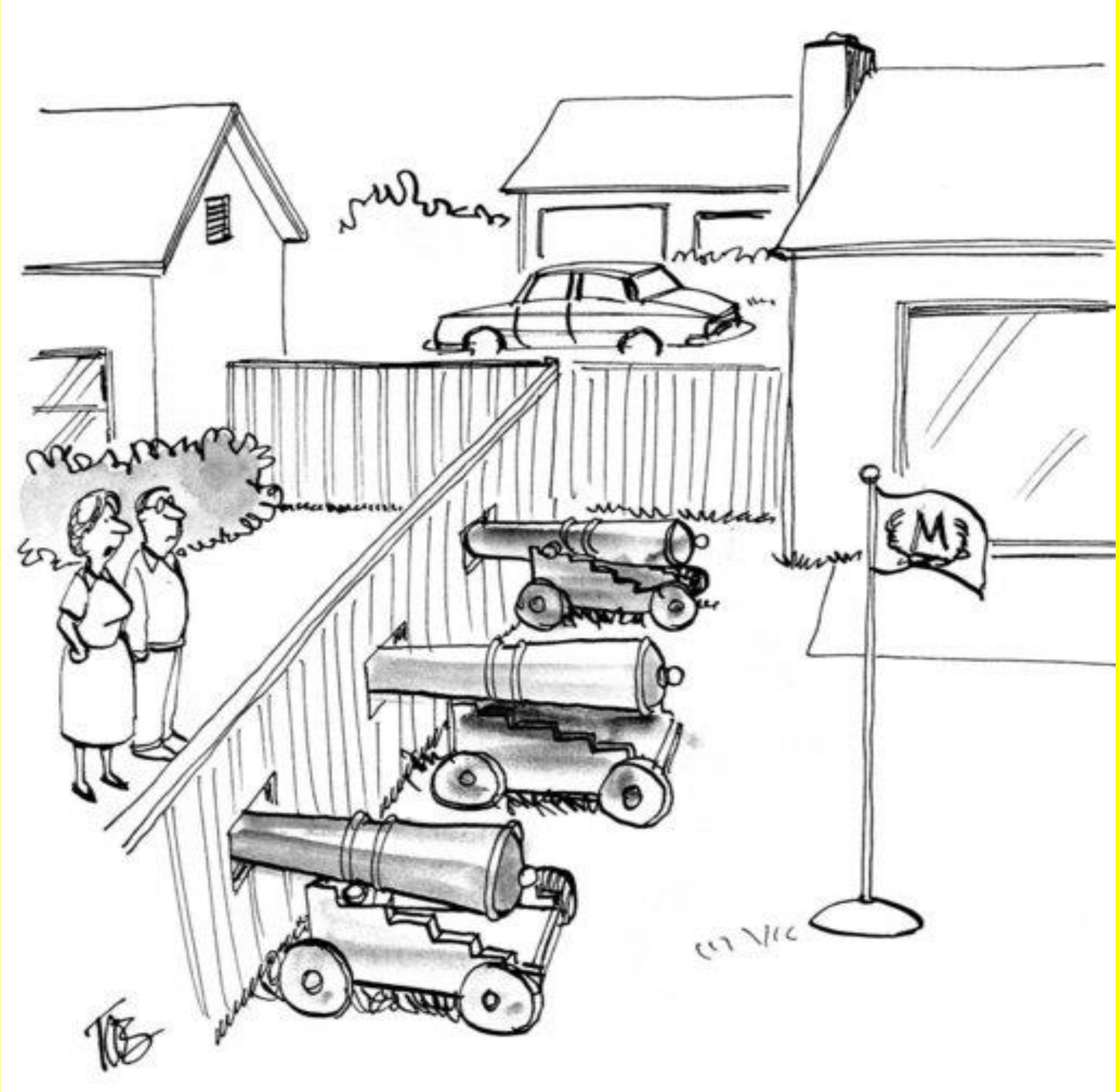
Laptops with 802.11 (2)

- Microsoft ActiveSync
  - Connect mobile PDAs, phones to host, NW
    - ✓Access e-mail
    - ✓Browse files
  - Can connect over WLAN
  - So attacker can use laptop as wireless proxy server
- Windows XP
  - Mesh NW (IBSS) allows connection from attacker's device to any corporate unit
  - Many people inadvertently share their C: drive by default
  - Even configure their firewall to allow share

Neighbors

- In cities, offices share buildings
- Can detect WLANs in adjacent buildings
- Attackers typically piggyback on other people's NWs
- Can also connect employees to wrong NW by mistake
  - Misuse of Internet bandwidth
  - Access to sensitive information
  - Vulnerability to sabotage
- Access by criminals can be serious
  - P2P file sharing or spamming can eat up bandwidth
  - Can also lead to criminal prosecution of victim of piggybacking
- Illegal ISP sharing
  - Some naïve users deliberately share their ISP connections to Internet (e.g., ADSL) using wireless router – violation of TOS (terms of service)
  - Can lead to civil prosecution for violation of contract

Neighbors

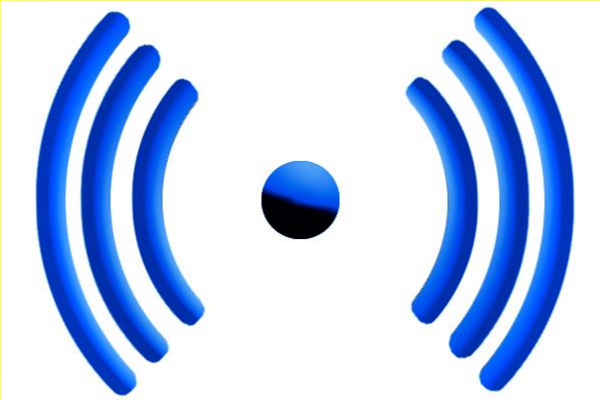


"Have we made a real effort to know the neighbors?"

Hot Spots

USE VPN TECHNOLOGY
See *CSH6* Chapter 32

- Many commercial access points in restaurants, coffee shops, bookstores, airports, conferences….
  - Completely open (no encryption)
  - Therefore allows capture of confidential unencrypted data
- Research at Planet Expo (Boston, 2003)
  - Tiny % wireless traffic encrypted
  - Significant criminal-hacker activity
    - ✓149 active war-driving scans
    - ✓105 DoS attacks
    - ✓32 attempted MITM attacks
- Airsnarf – example of program allowing criminal to become a rogue AP (steal user IDs, passwords)



Original 802.11 Functionality

- 2 security systems
  - 802.11 (1999) defined Wired Equivalent Privacy (WEP) – inadequate
  - 802.11i defined WPA (Wi-Fi Protected Access) & WPA2
- Topics
  - Security Functionality
  - Connecting to a Wireless Network & Authentication
  - Defending Against the WEP Vulnerability

Security Functionality

Original 802.11 standard provided for

- **Authentication – 2 different algorithms:**
  - **Open authentication**
  - **Shared-key authentication**
- **Confidentiality/privacy using WEP**
  - **Wired Equivalent Privacy**
  - **Encrypts data using keys on station**
- **Integrity**
  - **CRC-32 Integrity Check value (ICV)**
  - **CRC = *cyclic redundancy code***

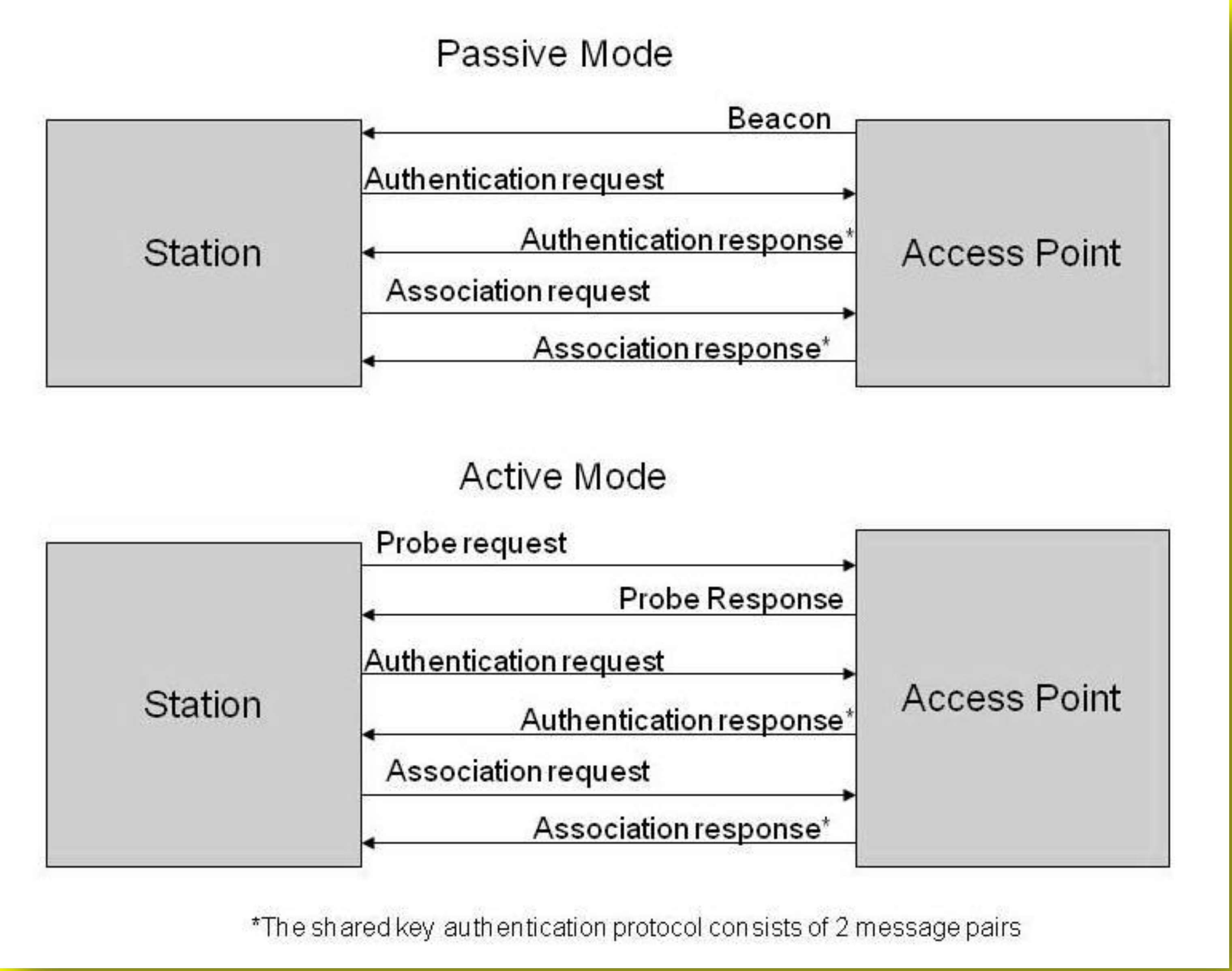
Connecting to a Wireless NW & Authentication (1)

NORWICH UNIVERSITY

- **Fundamental issue**
  - **Wired NWs can use physical controls to prevent / reduce unauthorized connections**
  - **Wired NWs must rely on protocol for defenses**
- **Overview**
  - **Sta* must 1st detect NW**
    - ✓ **Passive mode: listen for *beacon frames***
      - **Regularly transmitted by APs**
  - **Active mode: Sta sends *probe requests***
    - ✓ **Sta return *probe response***
    - ✓ **Often configure Sta to respond only to valid probe requests with valid NW identifier**

***Station**

Connecting to a Wireless NW & Authentication (2)



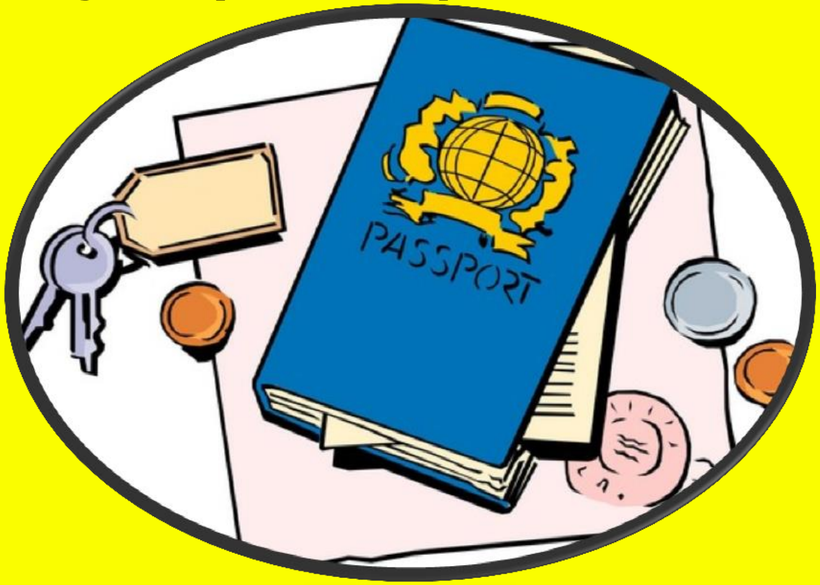
Connecting to a Wireless NW & Authentication (3)

Topics on following slides

- **Open Authentication**
- **Shared-Key Authentication**
- **WEP**
- **Fluhrer, Mantin & Shamir (FMS) Attack**
- **Developments Since the FMS Attack**

Open Authentication

- **Default mechanism in 802.11 (& only required 1)**
  - **Described as null algorithm**
  - **Sta provides identity**
  - **AP returns success or failure report**
  - **AP *does not attempt to verify identity* of Sta!**



- **Further refinements**
  - **Most implementations include ACL (*access control list*) in AP**
  - **Defines MAC (*media access control*) addresses for authorized Sta**
  - **But eavesdropper can capture MAC addresses & reprogram own Sta to *spoof authorized unit***

Shared-Key Authentication (SKA)

Optional protocol using WEP

1. Sta sends shared-secret key to AP
   - Contains IEEE MAC address
2. AP uses WEP to generate & return 128-byte random authentication challenge string
3. Sta copies challenge string into authentication data area in return message
   - Encrypts message using WEP
4. AP receives request from Sta

- Decrypts Sta request using WEP
- AP verifies ICV (integrity check value)
- Compares received challenge string with sent challenge string
- If both ICV & challenge string OK, sends *success*

Security Issues with SKA (1)

- Designers recognized flaws
- Both cleartext & encrypted versions of challenge string transmitted during negotiation
  - Thus attacker can capture both & crack pseudo-random number (PRN) sequence used to create authentication challenge (see previous slide)
  - "Implementations should therefore avoid using the same key/IV pair for subsequent frames."

- Borisov, Goldberg, & Wagner's analysis
  - SKA key stream established for each session between AP & specific Sta
  - But MITM attack can re-use fixed cryptographic elements without knowing original WEP key that starts process

Security Issues with SKA (2)

- **128 byte challenge can be re-used by Sta**
- **Therefore attacker can**
  - **Encrypt any string ≤ 128 bytes using known IV (initialization vector)**
  - **Inject messages into data stream**
  - **Can send commands (e.g., Ping) to generate more matching IVs & key streams**
  - **E.g., support dictionary attack on MACs**
- **RESULT:**

SKA PROTOCOL SHOULD NOT BE USED

WEP (Wired Equivalent Privacy)

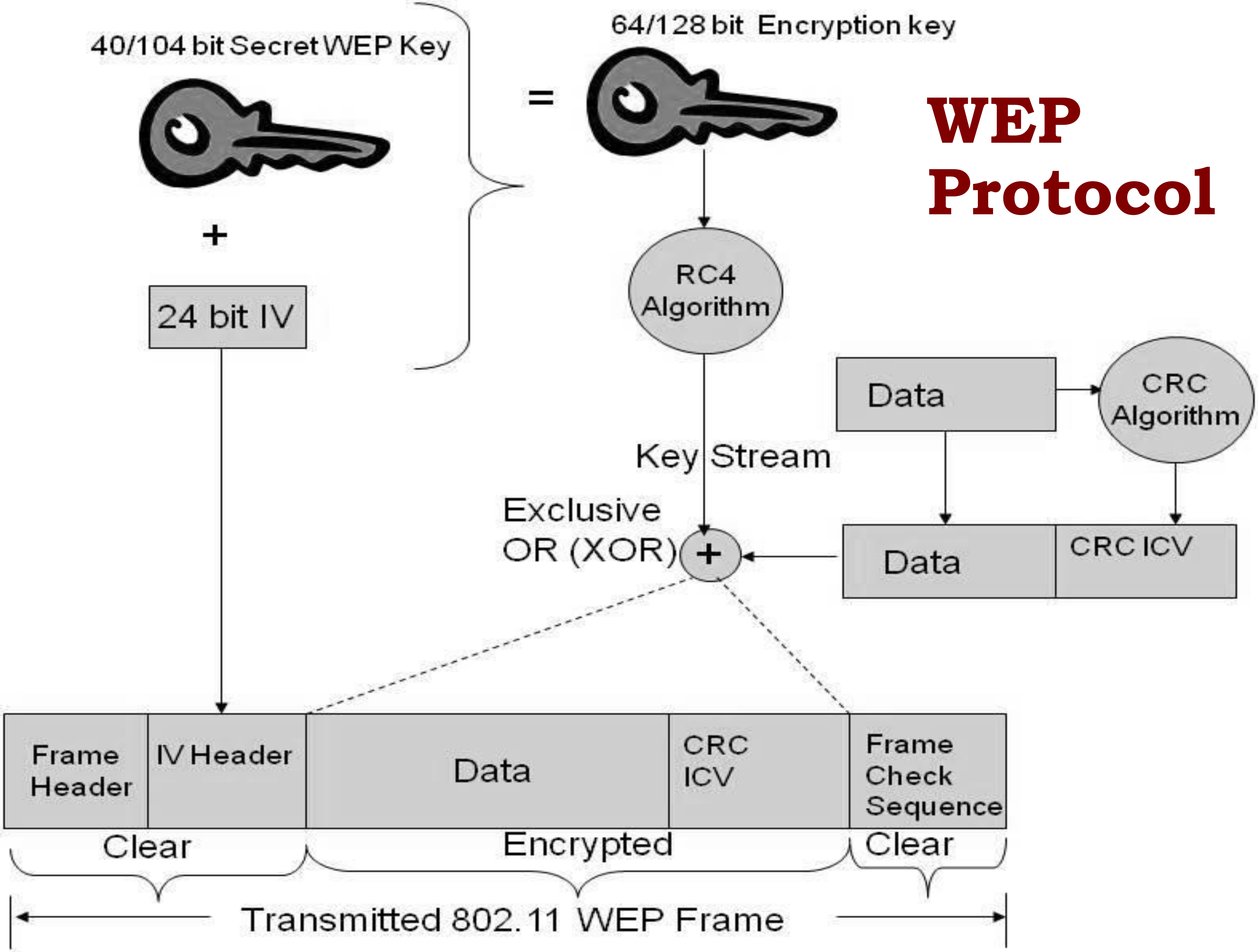
- **Defined in**
  - **IEEE 802.11b §8.2**
  - **Also in 802.11i**
- ***Topics on next slides***
  - **Properties of RC4 Stream Cipher**
  - **WEP Protocol**
  - **WEP Keys**
  - **Problems with WEP**
  - **Key Management**
  - **Problems with Key Management**
  - **Default WEP Keys**

Properties of RC4 Stream Cipher

- RSA (originally named for Rivest, Shamir & Adleman)
- RC4 = "Ron's Code" or "Rivest's Cipher" #4
  - Stream cipher
  - XOR key bytes with plaintext
  - No propagation of errors (unlike block ciphers)
- Stream ciphers vulnerable to known-plaintext attacks
  - Encrypt *known plaintext* with key
  - Then XOR *plaintext* with *ciphertext* to recover key stream
  - Can then insert spoofed messages using key

Ron Rivest

WEP Protocol



WEP Keys

- IEEE 802.11 stipulates 4 default keys for each Sta
  - Numbered 0, 1, 2, & 3
  - Each 40 bits
- Combine 1 of keys with 24-bit IV = 64-bit key
  - Used for RC4 computations as keystream
- But modern products use non-standard 104-bit keys
  - Combined with 24-bit IV = 128-bit key

Problems with WEP (Borisov, Goldberg & Wagner) (1)

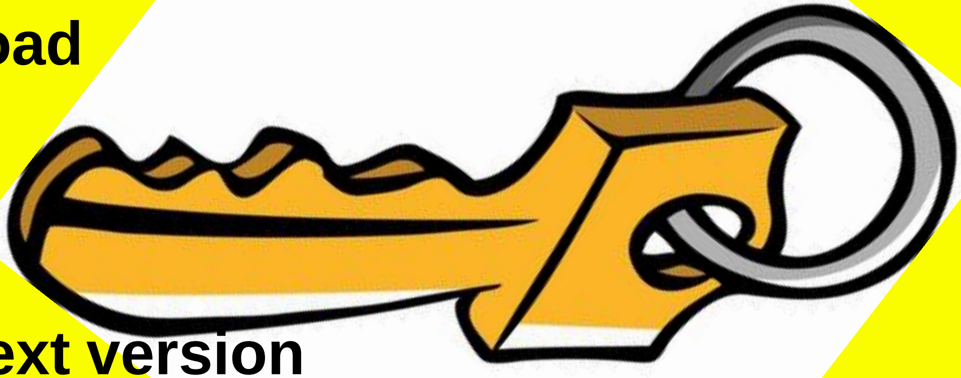
- **40-bit standard keys too short to prevent brute-force cracking (with today's CPU speeds)**
  - **Solved by de facto standard of 104-bit keys**
- **Key stream re-used**
  - **Therefore open to known-plaintext attacks**
  - **PLUS XOR of 2 separate ciphertexts encrypted by same stream cipher = 2 plaintexts XOR'd**
    - ✓ **Vulnerable to cryptanalysis**

- **No specified key management protocol**
  - **And *ad hoc* vendor-supplied KM protocols often weak**

(cont'd)

Problems with WEP (Borisov, Goldberg & Wagner) (2)

- **Replay attacks (message modification)**
  - **Demonstrated that encryption too weak to prevent changes in encrypted payload without altering checksum**
  - **So can inject altered payload**
- **Message injection**
  - **Obtain key stream by XORing known plaintext with its encrypted ciphertext version**
  - **Then XOR new message with key stream**
  - **Inject spoofed packets into data stream**
    - ✓ **Due to use of weak CRC-32 algorithm**
    - ✓ **Would be improved by using SHA-1 HMAC (hashed message authentication code)**



(cont'd)

Problems with WEP (Borisov, Goldberg & Wagner) (3)

NORWICH UNIVERSITY

- **IP redirection**
  - **Capture packet from Sta**
  - **Alter destination address to send to attacker's host on Internet**
  - **Attacker's host decrypts packet**
  - **Returns cleartext to attacker**
- **Reaction attack vs TCP**
  - **Flip one bit in captured TCP message**
  - **Send to TCP-based server**
  - **If TCP checksum still valid, server returns ACK; else no response**
  - **Thus server tests one bit at a time for cryptographic recovery of plaintext**

Key Management

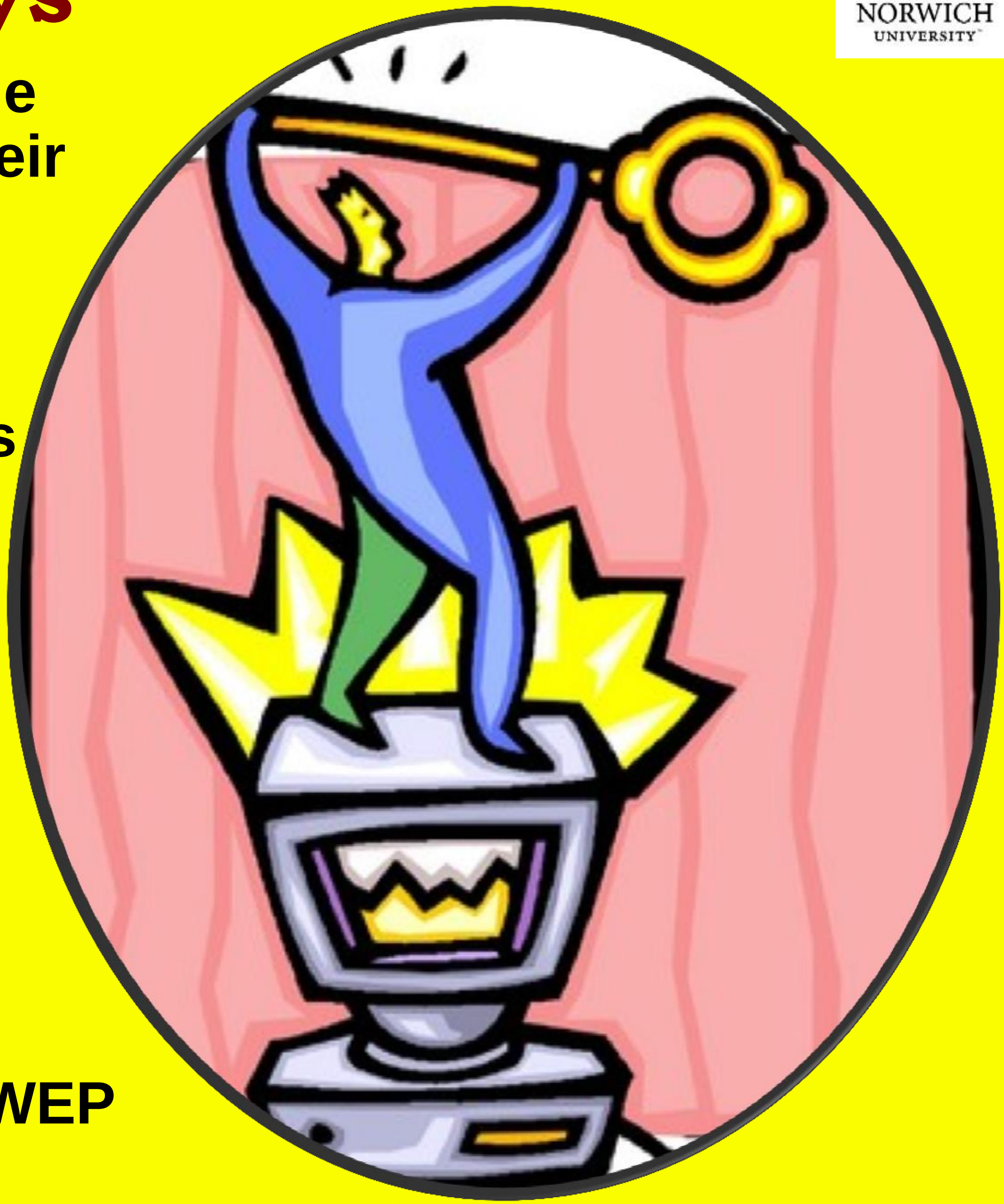
- Most WEP NWs use only 1 (the same) shared key (out of only 4) for all Sta
- Increases chances of integrity value (IV) collisions & re-use of IV in attacks
- Lack of prescribed KM protocol has led to vendor- or implementation-specific protocols
- Many vendors rely on manual system to define keys – not manageable or scalable

Problems with Key Management

- Keys manually entered into each Sta
  - Many products display keys in plaintext
  - So then many people get to know the keys
- Difficult or impossible to coordinate change of keys
  - So many installations never change their keys at all
  - Thus attackers have lots of time for cryptanalysis
  - Former staff may know long-standing keys after departure from organization

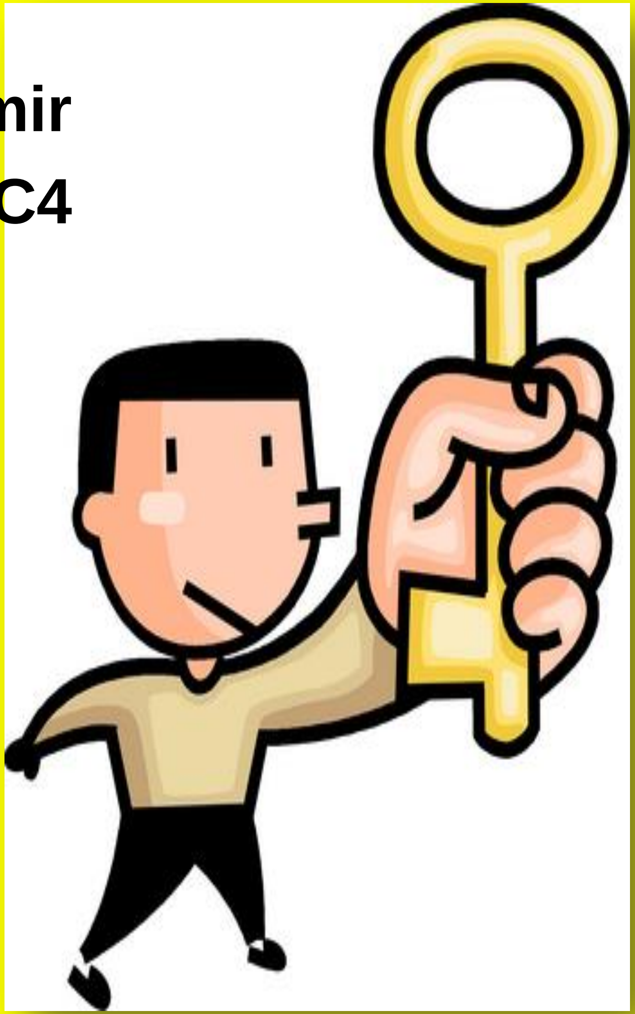
Default WEP Keys

- Many manufacturers code default WEP keys into their equipment
- Equivalent to canonical passwords in other access-control situations such as application programs
- Attackers well familiar with default values
  - Netstumbler & Kismet identify manufacturer
  - Easy to enter known keys to break into NW
- DO NOT USE DEFAULT WEP KEYS!



Fluhrer, Mantin & Shamir (FMS) Attack (Aug 2001)

- **Scott Fluhrer, Itsik Mantin & Adi Shamir**
- **Published paper on weaknesses in RC4**
  - **Speculated on attacking WEP**
- **Adam Stubblefield, John Ioannidis, & Ariel Rubin (Aug 2001)**
  - **Described successful attack**
  - **Took only 2 hours to write script**
  - **Took few days to gather OTS HW & SW to recover WEP key**
  - **Need to collect ~5M packets (or as few as 1M)**
  - **Airsnort & WEPCrack use this attack method**



Developments Since the FMS Attack

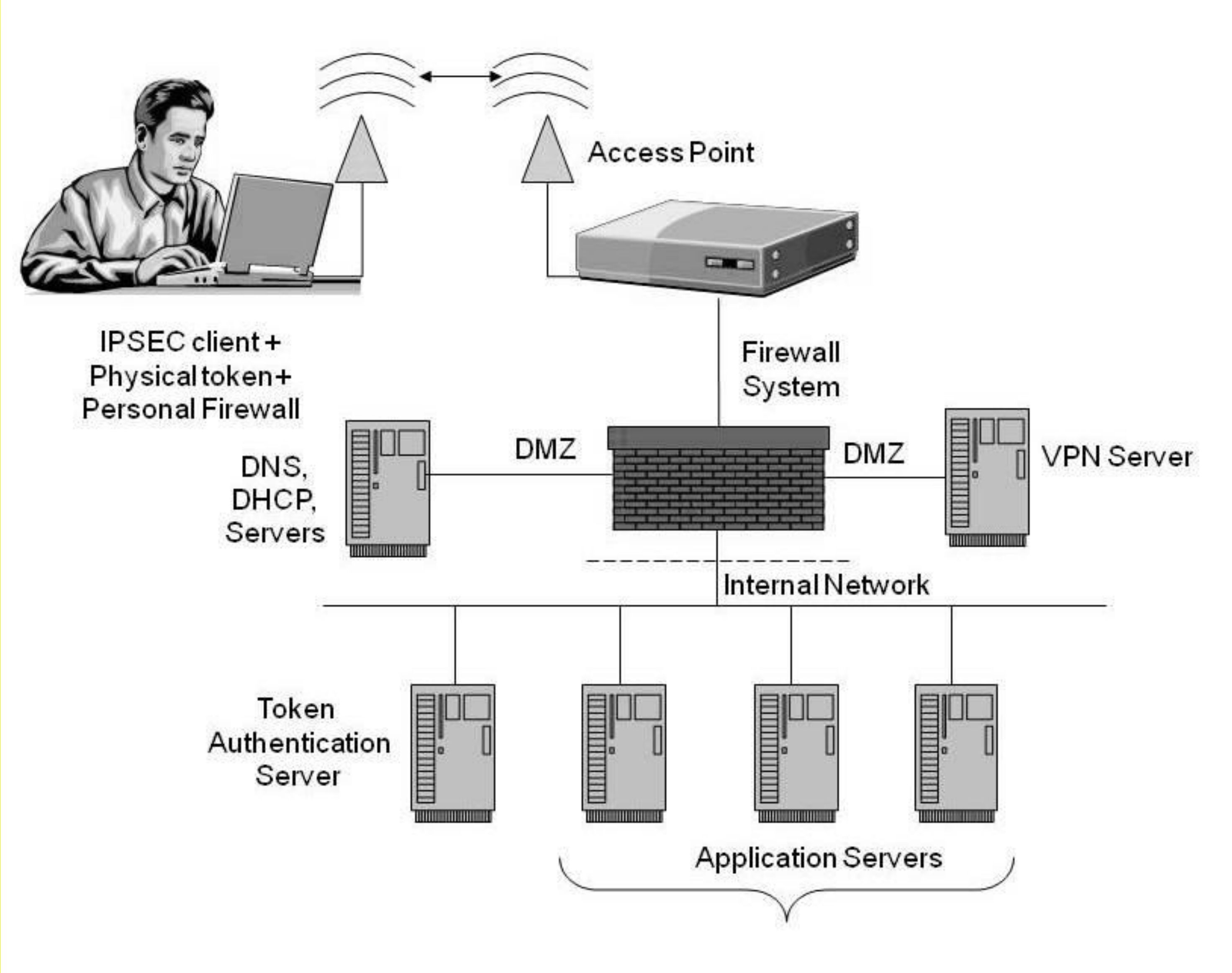
- **Vendors responded to FMS & SIR papers**
  - **Dropped weak initialization vectors (IVs)**
  - **Developed new protocol: Dynamic WEP (see later)**
- **But attackers quickly undermined all WEP security**
  - **Aug 6, 2004: "Korek" posted *chopper***
    - ✓**Statistical attack does not depend on weak IVs**
    - ✓**Requires only 100Ks of packets**
    - ✓**Integrated into Airsnort & Aircrack tools**

(cont'd)

Defending Against WEP Vulnerabilities (1)

- **Best defense: don't use WEP at all!**
  - **Use 802.11i WPA (Wi-Fi Protected Access) or WPA2**
- **If you must use WEP, see Exhibit 33.7 in *CSH6* (p 33.21) for list of problems & countermeasures**
- **Exhibit 33.8 (next slide) summarizes safe topology for wireless networks using WEP**
  - **Note firewall between WAP & all other network components**
- **Further topics discussed below**

Defending Against WEP Vulnerabilities (2)



Defending Against the WEP Vulnerabilities (3)

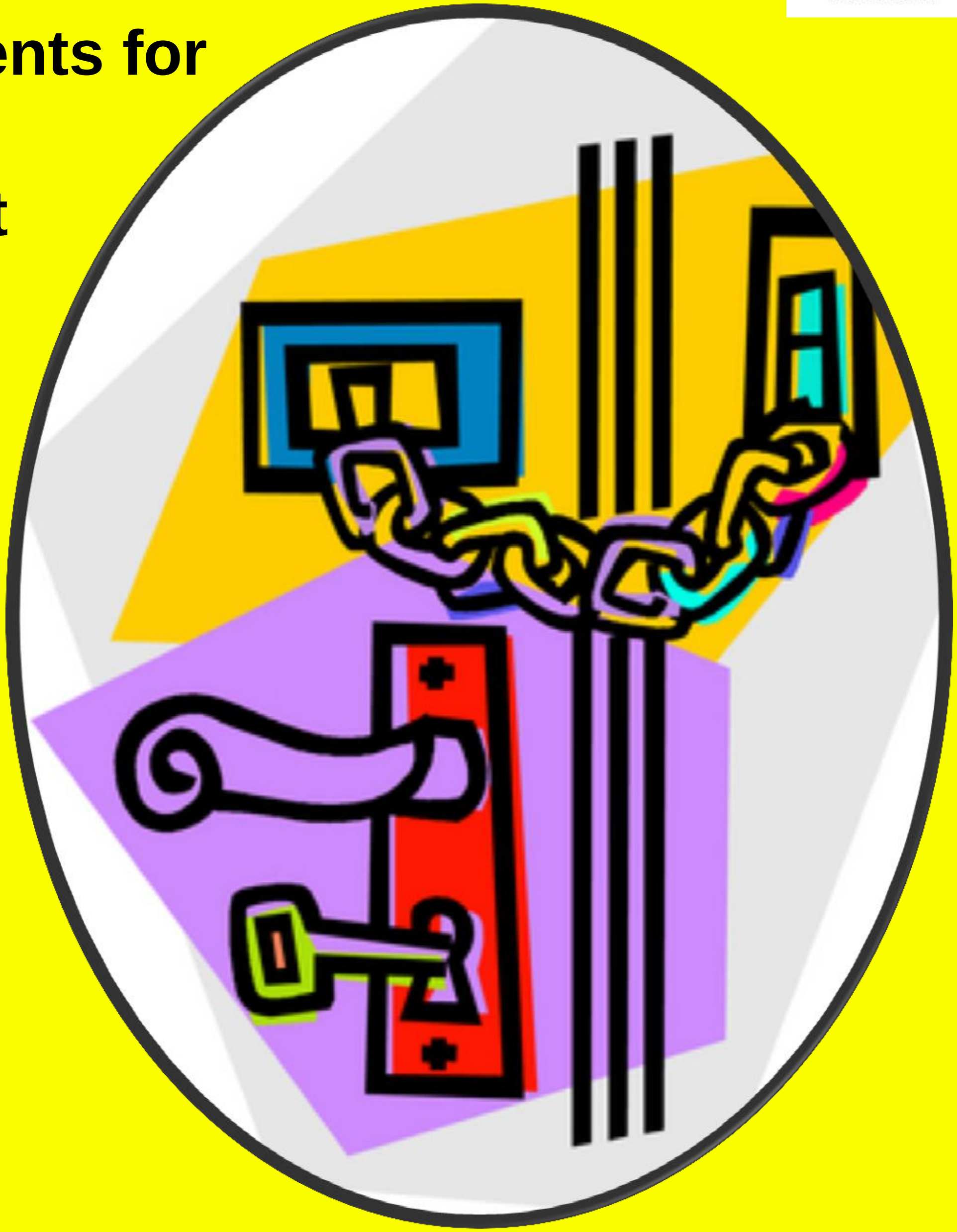
NORWICH UNIVERSITY

Further topics

- **Additional Crucial Controls**
- **VPN & WEP**
- **AP Configuration**
- **AP Location**
- **Dynamic WEP**
- **Concluding Remarks on WEP**
- **Resolving Implementation & Operational Problems**
- **Remote Access & Public WAPs**

Additional Crucial* Controls

- Necessary procedural elements for WLAN security
- Effective patch management
- Regularly updated antimalware solution
  - Antivirus
  - Antispyware
- Only security-policy-compliant Sta may be connected to WLAN
  - Firewall
  - Patches
  - Antimalware



VPN & WEP

- **Should one use WEP with a VPN?**
- **Not strictly necessary because VPN handles encryption satisfactorily**
- **But attackers may see NW without WEP as potentially unprotected**
  - **Can probe for weaknesses**
  - **Could launch / cause DoS**
- **So WEP serves as deterrent**
  - **Remember story of two hikers chased by grizzly**
  - **"This is crazy! We can't outrun a grizzly bear!"**
  - **"I don't have to outrun the grizzly: I just have to outrun *you*."**

AP Configuration

- Some WLANs configured to suppress SSID broadcast & not respond to broadcast probes
  - Theory is *security by obscurity*
  - Windows XP & simple war-driving tools (e.g., Netstumbler) will not see NW
- But more sophisticated attacker monitors actual traffic
- So these measures may cause more inconvenience for legitimate users than for attackers
- General principle: run secure WLAN & no unauthorized user will be able to join NW

AP Location

- Physical location of AP affects signal strength
- Places to position AP for better security:
  - Middle of room
  - 1st or 2nd floor of building
- Places to avoid placing AP:
  - Outside (street-facing) walls
  - Upper floors

Dynamic WEP

- Vendors introduced dynamic WEP keys
  - Established in 802.1x authentication exchange
  - Every Sta has own WEP key
  - AP changes key regularly
- Standard option in Windows XP client
  - "This key is provided for me automatically"
- Evaluation
  - Massive improvement over static WEP keys
  - But does not defend against active WEP attacks
- Recommendations
  - Use dynamic WEP keys BUT
  - Plan to move to more secure WPA or WPA2

Concluding Remarks on WEP

- “WEP is fundamentally broken.”
- New attacks constantly generated
- Avoid WEP if possible
- Use WPA or WPA2
- Or encrypt data (VPN) using IPSec or SSL

Resolving Implementation & Operational Problems

- Plan for security breaches
- Defend each component of NW
- Do not allow use of default configurations & default keys
- Recommendations
  - Issue corporate policy on WLANs
  - Publicize & enforce policy
  - Develop approved WLAN
    - ✓Architecture
    - ✓Configuration standards
    - ✓Operating procedures

"By the way, what's the office policy on smoking?"

Remote Access & Public WAPs

- **Unsecured home network may circulate unencrypted traffic**
  - **So connecting unsecured network to corporate systems using encrypted links will still not protect data**
  - **Therefore use VPNs for connection to corporate NW**

- **But rogue hot spots dangerous**
  - **Criminal's AP spoofs legitimate AP**
  - ***Before* establishing VPN**
- **Vendors working to implement secure protocols in *hardware***

Wi-Fi Alliance's WPA & WPA2 Standards

- **Wi-Fi Alliance**
  - **Non-profit organization**
  - **Certify interoperability of 802.11 products**
  - **Concerned about security weakness of WEP**
- **Created Wi-Fi Protected Access (WPA)**
  - **Subset of 802.11i (see §33.5 – not included in this IS340 curriculum and these slides)**
  - **Uses Temporary Key Integrity Protocol (TKIP, see §33.5 33.5.5 for details)**
  - **Vulnerable to offline dictionary attack**
- **WPA2 is equivalent to complete 802.11i**
  - **See Wi-Fi Alliance white papers at http://www.wi-fi.org**

802.11 Security Auditing Tools (1)

- Auditor & BackTrack
- Kismet
- Netstumbler
- Airsnort (old)
- CoWPAtty & Aircrack
- Ethereal
- Wellenreiter
- Commercial Wireless Auditing Tools

802.11 Security Auditing Tools (2)

- More detail than appropriate for IS340
- See Exhibit 33.19 for synoptic table
- Read §33.6 for details

Now go and study