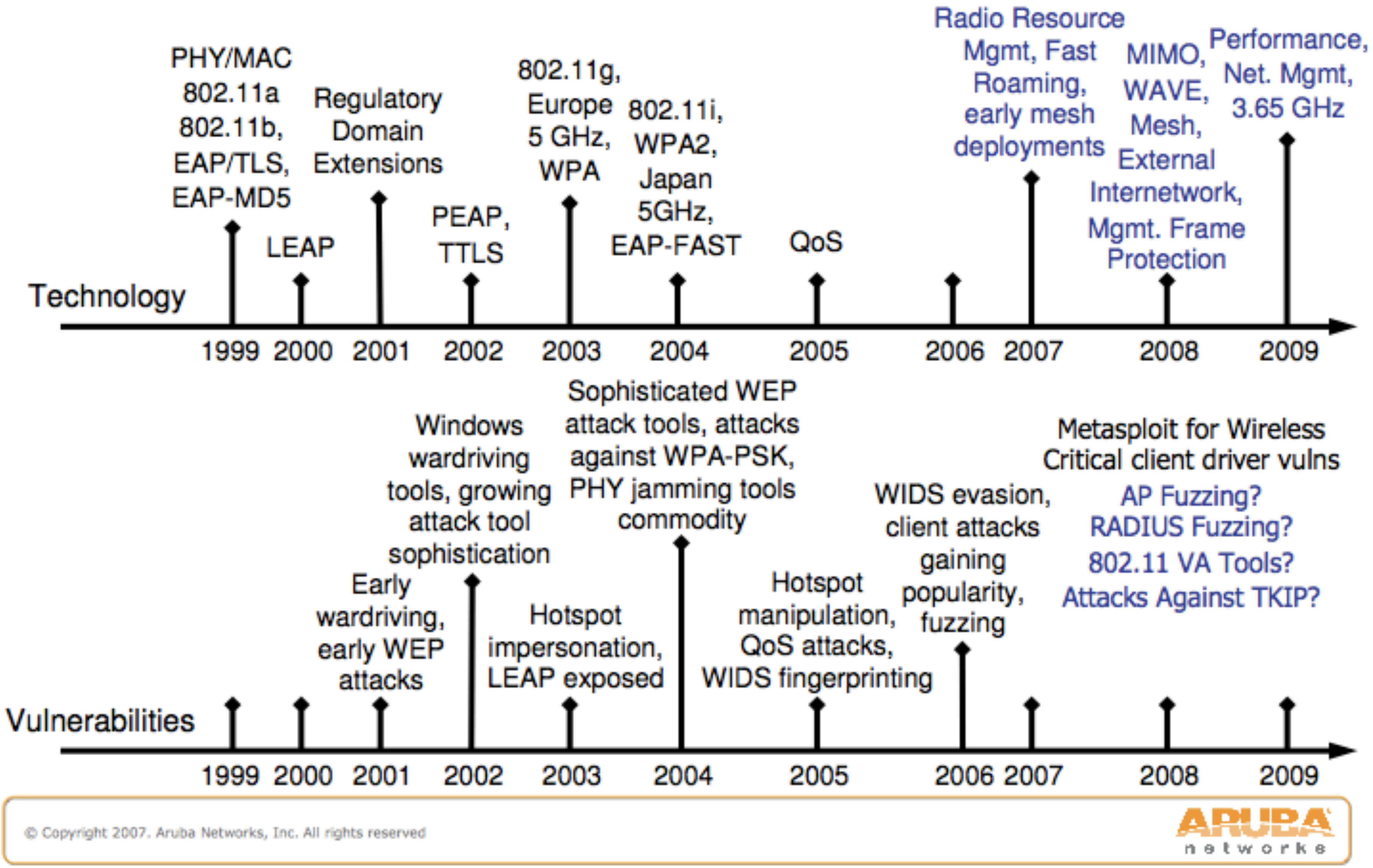
Last Lecture: Data Link Layer

1. *Design goals and issues*
2. *(More on) Error Control and Detection*
3. *Multiple Access Control (MAC)*
4. *Ethernet, LAN Addresses and ARP*
5. *Hubs, Bridges, Switches*
6. *Wireless LANs*
7. Mobile Networking ✔
8. WLAN Security

This Lecture: Data Link Layer

1. *Design goals and issues*
2. *(More on) Error Control and Detection*
3. *Multiple Access Control (MAC)*
4. *Ethernet, LAN Addresses and ARP*
5. *Hubs, Bridges, Switches*
6. *Wireless LANs*
7. Mobile Networking
8. WLAN Security ✓

802.11 Technology and Vulnerabilities



Technology

1999: PHY/MAC 802.11a 802.11b, EAP/TLS, EAP-MD5

2000: LEAP

2001: Regulatory Domain Extensions

2002: PEAP, TTLS

2003: 802.11g, Europe 5 GHz, WPA

2004: 802.11i, WPA2, Japan 5GHz, EAP-FAST

2005: QoS

2006

2007: Radio Resource Mgmt, Fast Roaming, early mesh deployments

2008: MIMO, WAVE, Mesh, External Internetwork, Mgmt. Frame Protection

2009: Performance, Net. Mgmt, 3.65 GHz

Vulnerabilities

1999

2000

2001: Early wardriving, early WEP attacks

2002: Windows wardriving tools, growing attack tool sophistication

2003: Hotspot impersonation, LEAP exposed

2004: Sophisticated WEP attack tools, attacks against WPA-PSK, PHY jamming tools commodity

2005: Hotspot manipulation, QoS attacks, WIDS fingerprinting

2006: WIDS evasion, client attacks gaining popularity, fuzzing

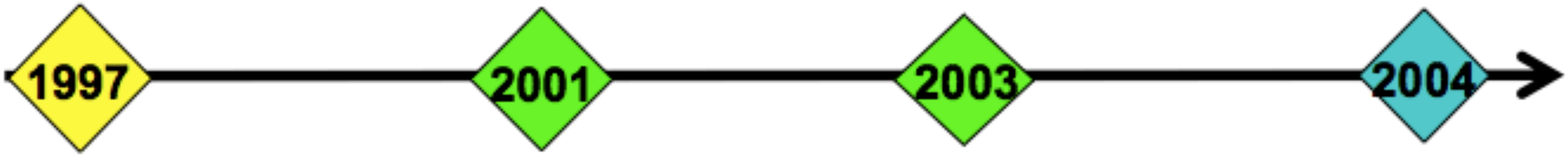
2007

2008: Metasploit for Wireless Critical client driver vulns

2009: AP Fuzzing? RADIUS Fuzzing? 802.11 VA Tools? Attacks Against TKIP?

ARUBA networks

Evolution of 802.11 Security Standards



Original 802.11 Security:

- Native 802.11 authentication
- WEP encryption

WEP issues documented October 2000-August 2001

802.1X with WEP

- 802.1X authentication
- 802.1X key rotation
- WEP data protection

WPA = pre-standard subset of 802.11i

- 802.1X authentication
- 802.1X key management
- TKIP data protection

802.11i

- 802.1x authentication
- enhanced 802.1X key management
- AES-based data protection
- enhanced support infrastructure
- Ratified June 23

Evolution of 802.11 Security Standards

- 1997 the original 802.11 standard only offers
  - SSID (Service Set Identifier)
  - MAC Filtering (Media Access Control)
  - and WEP (Wired Equivalent Privacy)
- 1999 WECA formed for rapid adaption of 802.11
- 2000 Jesse Walker (Intel)
  - "Unsafe at any keysize; An analysis of the WEP encapsulation"
- 2001 *the FMS attack pretty much demolished WEP*
  - Scott Fluhrer, Itsik Mantin, Adi Shamir; "Attacks on RC4 and WEP: Weaknesses in the Key Scheduling Algorithm of RC4"
  - Tools available: WEPCrack, AirSnort

Evolution of 802.11 Security Standards

- 2002
  - WECA was renamed *Wi-Fi Alliance*
  - Cisco developed *LEAP* authentication protocol
- 2003 Wi-Fi Protected Access (WPA) introduced
  - Supposed to be an interim solution for WEP problems
  - Some parts of IEEE 802.11i
  - WPA-PSK, WPA-RADIUS
  - Josh Wright discovered LEAP attack, ASLEEP released
- 2004 WPA2 was introduced
  - Based on the final IEEE 802.11i standard
  - Was ratified on June 25
  - Cisco released AEP-FAST (to replace LEAP)

WEP/WPA Attacks

- Tons of other WEP attacks, get through in 1 min
  - 2004, KoreK. Next generation of WEP attacks?
    http://www.netstumbler.org/ showpost.php?p=93942&postcount=35
    KoreK. chopchop (experimental WEP attacks). http://www.netstumbler.org/ showthread.php?t=12489, 2004.
  - 2007, PTW attack
    Erik Tews, Ralf-Philipp Weinmann, Andrei Pyshkin. Breaking 104 bit wep in less than 60 seconds
    Erik Tews. Attacks on the wep protocol. Cryptology ePrint Archive, Report 2007/471, 2007
  - 2008, Beck-Tews attack
    http://dl.aircrack-ng.org/breakingwepandwpa.pdf
- WPA attacks too
  - 2003, WPA-PSK weakness Robert Moskowitz , "Weakness in Passphrase Choice in WPA Interface"
  - 2008, Beck-Tews http://dl.aircrack-ng.org/breakingwepandwpa.pdf
  - 2009, An Improved Attack on TKIP
- A **ton** of tools for script-kiddies
  - AirCrack-ng, aircrack-ptw, Wtoolkit, Airbase, Kismet, AirPWN, KARMA, Metasploit

Brief Comparisons of The Standards

	WEP	WPA	WPA2
○ Cipher	RC4	RC4	AES
○ Key Size	40 or 104bits	104bits perPack	128bits encry.
○ Key Life	24bit IV	48bit IV	48bit IV
○ Packet Key	Concatenation	TwoPhaseMix	Not Needed
○ Data Integrity	CRC32	Michael MIC	CCM
○ Key Mngmt.	None	802.1X/EAP/PSK	802.1X/EAP/PSK

Some Headlines

- 2002 (http://www.securityfocus.com/columnists/167)
  - Stefan Puffer, a Houston computer security consultant, conducted a "*war driving*" exercise, reportedly accompanied by the head of Harris County's Central Tech. Dept., and a reporter for the Houston Chronicle.
  - Puffer demonstrated that the Harris County clerk's office's 802.11b network was mis-configured to allow anyone to have access to the network.
  - For his efforts, Puffer was … investigated by FBI agents, who kicked in his door at 6AM, seized his computers and all electronic media and effectively put him out of business.
  - Then he was indicted by a federal grand jury for violating the federal Computer Fraud and Abuse Act -- with the "damages," bizarrely, assessed as the money the county spent to close the security hole.
  - Puffer eventually had to stand trial -- at a cost of tens of thousands of his own and taxpayer dollars.
  - The jury acquitted him in 15 minutes.

Some Headlines

- 2002: Best Buy
  - http://www.computerworld.com/s/article/70840/Holes_expose_retail_data?taxonomyId=009
  - Discussion on public mailing lists reveals merchant transmits credit card numbers on unencrypted WLAN in stores
  - Best Buy removes 493 store WLANs
  - No charges filed, no estimate on number of credit card numbers exposed to passive WLAN listeners

Some Headlines

- 2004: BJ’s Wholesale Club
  - http://www.computerworld.com/s/article/91412/Credit_card_data_breach_probed_at_BJ_s_stores
  - Wholesale merchant reports that a "small fraction" of its 8-million customers may have had CC#'s stolen
  - FTC asserts charges against BJ's for *unencrypted wireless networks*, default usernames/passwords and insufficient monitoring
  - BJ's settles, recording $10M in legal costs, agrees to thorough external audits every other year for 2 decades

Some Headlines

- 12/16/2004 http://www.securityfocus.com/news/10138
  - *"A 21-year-old Michigan man was sentenced to nine years in federal prison Wednesday in federal court in Charlotte, North Carolina for his role in a failed scheme to steal credit card numbers from the Lowe's chain of home improvement stores by taking advantage of an unsecured wi-fi network at a store in suburban Detroit."*
  - 2003: Botbyl was "wardriving" and stumbled across an unsecured wireless network at the Southfield, Michigan Lowe's
  - Later, they used the wireless network to route through Lowe's corporate data center in North Carolina and connect to the local networks at stores in Kansas, North Carolina, Kentucky, South Dakota, Florida, and two stores in California. At two of the stores -- in Long Beach, California and Gainseville, Florida -- they modified a proprietary piece of software called "tcpcredit" that Lowe's uses to process credit card transactions, building in a virtual wiretap that would store customer's credit card numbers where the hackers could retrieve them later.

Some Headlines

- 6/2005: GE Money
  - http://www.computerworld.com/s/article/104005/Finns_urge_better_Wi_Fi_security_after_bank_break_in
  - “*Finland called on its citizens to take more care securing their Wi-Fi networks after news emerged this week that about $245,400 (U.S.) had been stolen from a local bank using an unprotected home network.*” ☺
  - Investigators traced attack to unprotected consumer WLAN. Further investigation reveals GE Money data security manager and accomplices stole account information

Some Headlines

- 1/2007: TJX
  - http://wifinetnews.com/archives/2007/05/marshalls_use_of_wep_leads_to_200m_stolen_credit_card_number.html
  - Marshalls department store in St. Paul Minnesota WEP-protected WLAN compromised
  - Estimates between 45.7 million and 200 million payment card numbers revealed, 451,000 drivers licenses and SS#'s also compromised. Forrester Research estimates the cost of the breach couldsurpass 1 billion dollars in 5 years
  - “TJX declined to comment on those numbers, but says it is undertaking a "thorough, painstaking investigation of the breach," [...] It says it will also pay for a credit-card fraud monitoring service to help avert identity theft for customers whose Social Security numbers were stolen. "*We believe customers should feel safe shopping in our stores*," says a letter from Chief Executive Carol Meyrowitz posted on TJX's Web site.”

Some Headlines

- 2007
  - http://www.theregister.co.uk/2007/09/12/max_vision_faces_more_hacking_charges/
  - Max Butler stole thousands of credit card numbers
  - Witnesses told agents that Butler moved to various hotel rooms where he would use a high-powered antenna to intercept wireless communications, the AP reports. He would use the information obtained to hack into the institutions. One witness said Butler gained access to the *Pentagon Federal Credit Union, Citibank* and a government employee's computer.

Basic Problems

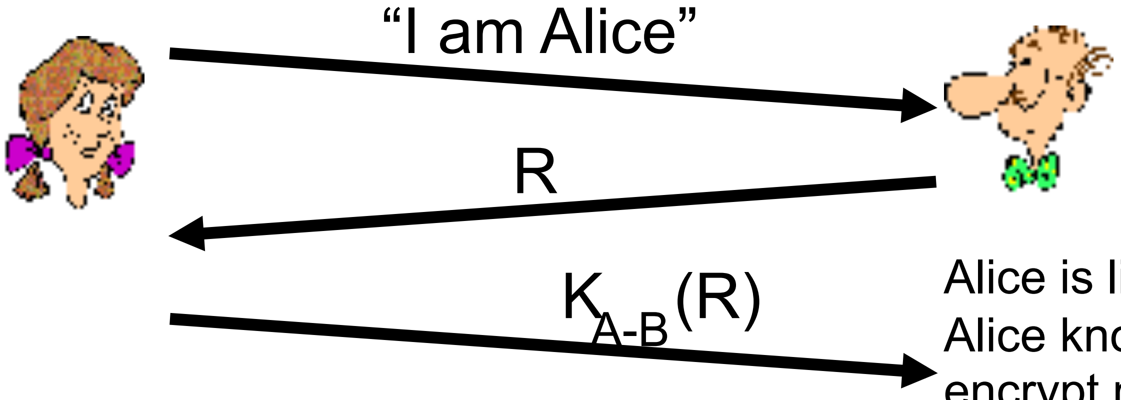
- *Authentication*
  - Only allow certain users to access the network
- *Data integrity*
  - Ensures data is not modified
- *Confidentiality*
  - Prevent eavesdropping

Basic WLAN Authentication Methods

- *SSID "hiding"*
  - Disable broadcast beacon (choose "don't broadcast")
  - SSIDs are sent anyhow in other frames
    - Probe requests, Probe responses, Association requests, Re-association requests
- *MAC address filter*
  - Only allow listed MACs to associate
  - A hassle to manage
  - MACs are sent in clear texts anyhow
- *WEP Shared Key Authentication*

Shared Key Authentication

- Shared Key Authentication
  - AP & users share a key



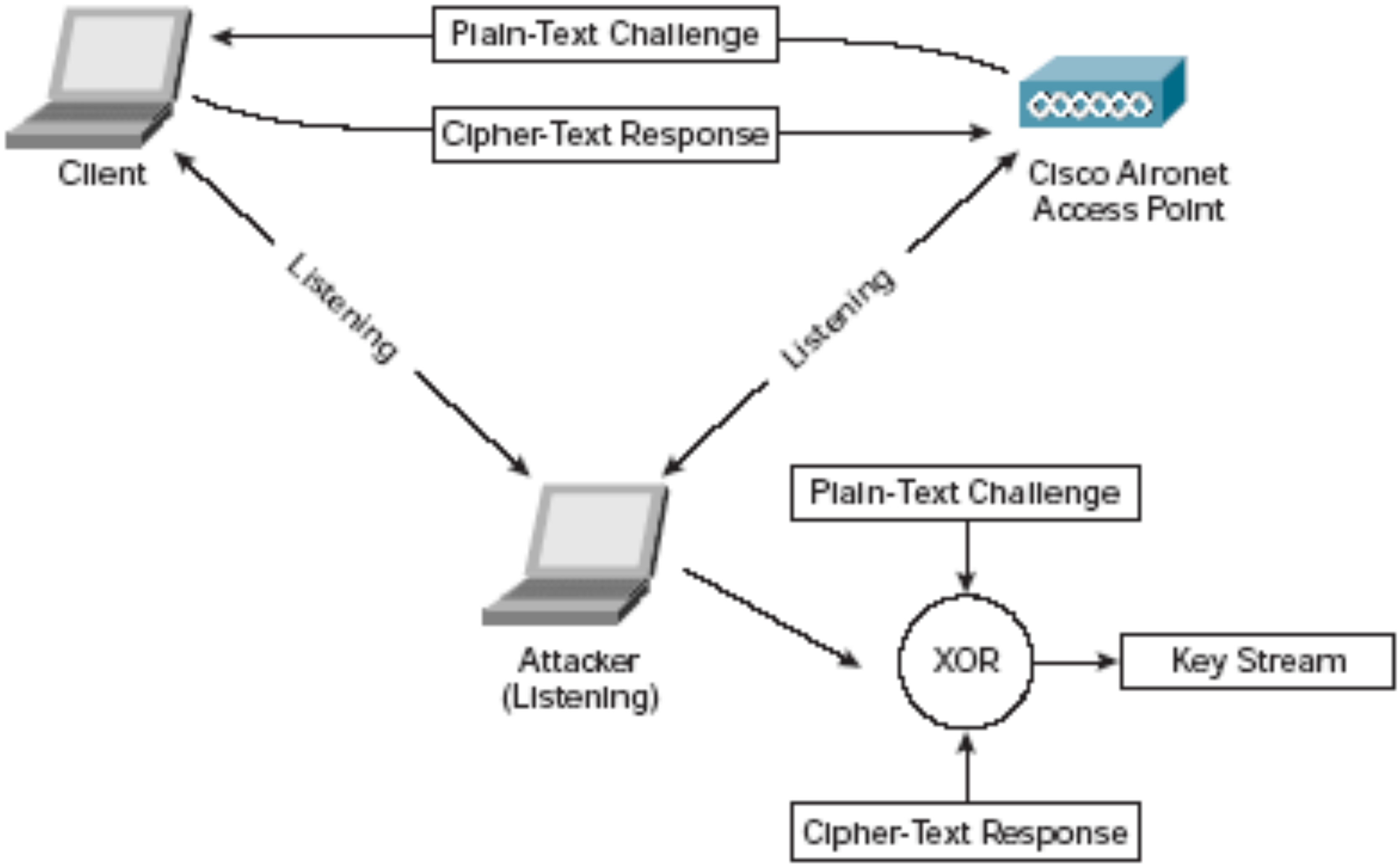
“I am Alice”

R

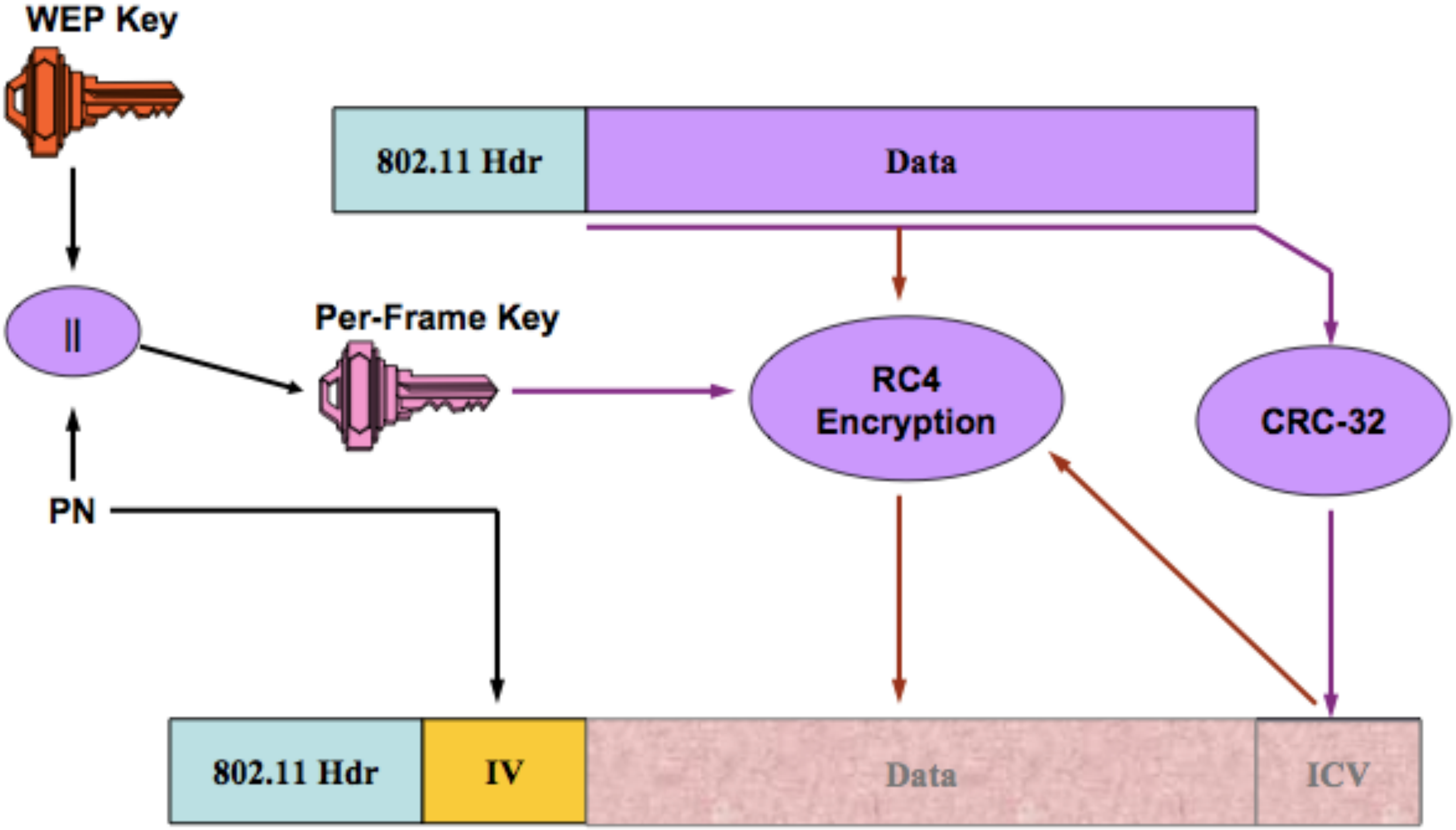
$K_{A-B}(R)$

Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

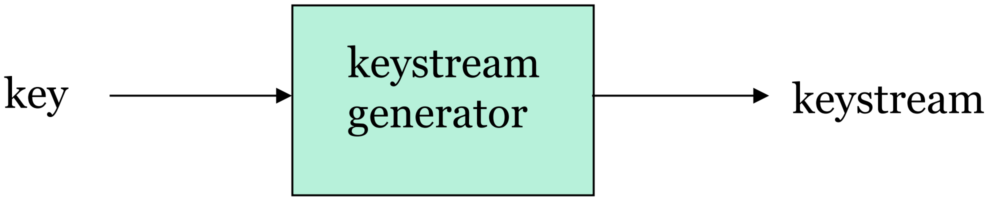
Problem with Shared Key Authentication



WEP Description



Review: Symmetric Stream Ciphers

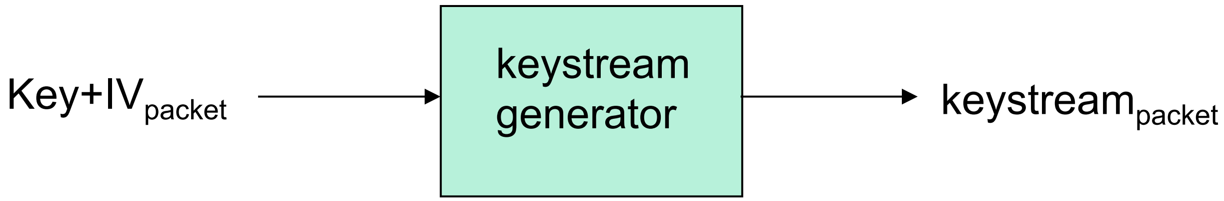


WEP uses RC4

- Combine each byte of *keystream* with byte of *plaintext* to get *ciphertext*
- m(i) = ith unit of message
- ks(i) = ith unit of keystream
- c(i) = ith unit of ciphertext
- $c(i) = ks(i) \oplus m(i)$ ($\oplus$ = exclusive or)
- $m(i) = ks(i) \oplus c(i)$

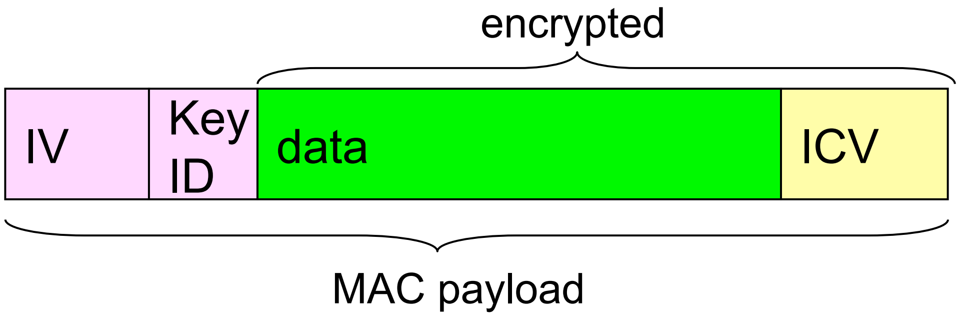
Stream cipher and packet independence

- Want each packet separately encrypted
- If for frame n+1, use keystream from where we left off for frame n, then each frame is not separately encrypted
  - Need to know where we left off for packet n
- WEP approach: initialize keystream with key + new IV for each packet:

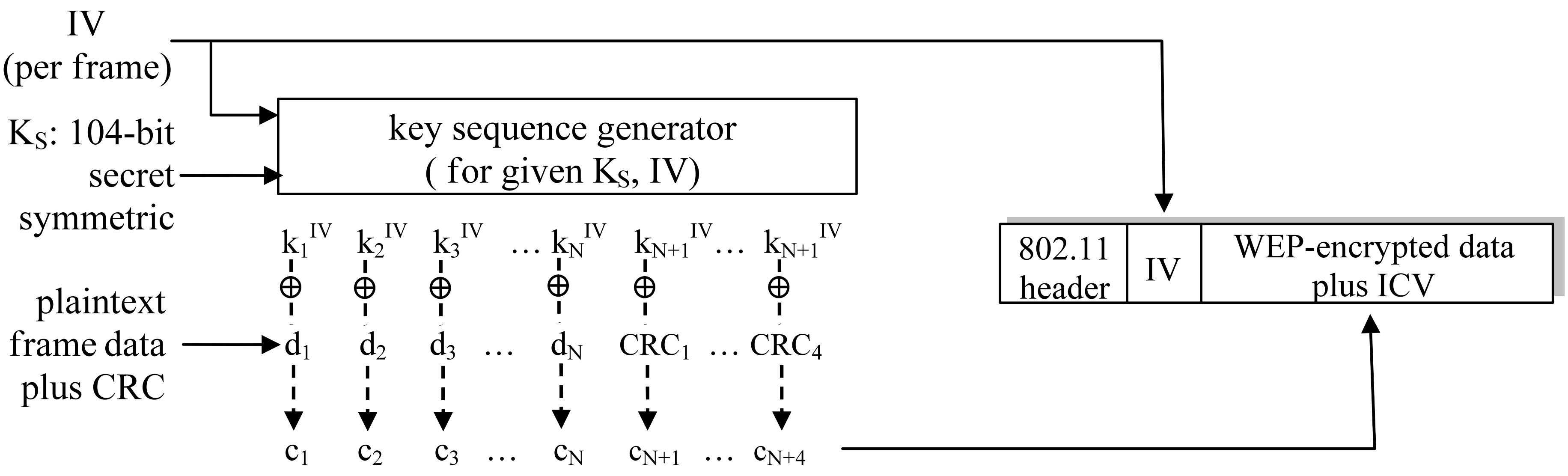


WEP encryption (1)

- Sender calculates Integrity Check Value (ICV) over data
  - four-byte hash/CRC for data integrity
- Each side has 104-bit shared key
- Sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key
- Sender also appends keyID (in 8-bit field)
- 128-bit key inputted into pseudo random number generator to get keystream
- data in frame + ICV is encrypted with RC4:
  - Bytes of keystream are XORed with bytes of data & ICV
  - IV & keyID are appended to encrypted data to create payload
  - Payload inserted into 802.11 frame



WEP encryption (2)



IV
(per frame)

K_S: 104-bit
secret
symmetric

key sequence generator
(for given K_S, IV)

plaintext
frame data
plus CRC

k_1^{IV} k_2^{IV} k_3^{IV} … k_N^{IV} k_{N+1}^{IV} … k_{N+1}^{IV}

$\oplus$ $\oplus$ $\oplus$ $\oplus$ $\oplus$ $\oplus$

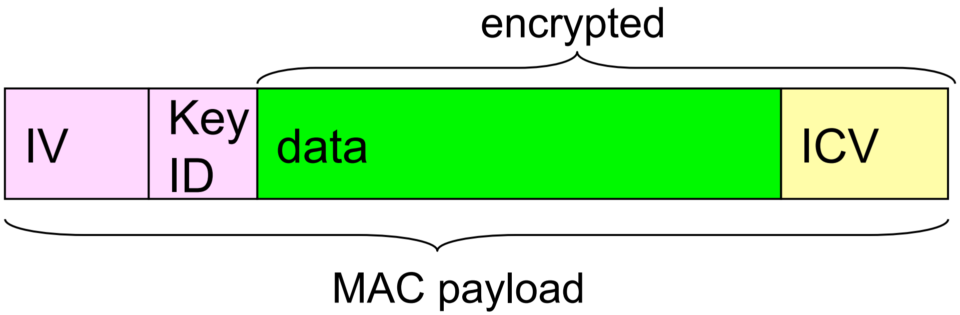
d_1 d_2 d_3 … d_N CRC_1 … CRC_4

c_1 c_2 c_3 … c_N c_{N+1} … c_{N+4}

802.11 header	IV	WEP-encrypted data plus ICV

New IV for each frame col

WEP decryption overview



- Receiver extracts IV
- Inputs IV and shared secret key into pseudo random generator, gets keystream
- XORs keystream with encrypted data to decrypt data + ICV
- Verifies integrity of data with ICV
  - Note that message integrity approach used here is different from the MAC (message authentication code) and signatures (using PKI).

WEP Weaknesses

- Key Management and Key Size (40 bit)
  - No key management: keys tend to be long-lived!
- The Initialization Vector (IV) is Too Small
  - WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size.
  - AP with 1500Byte/packet and 11Mbit/s: must recycle after 1500*8/(11*10^6)*2^24=18300sec ~ 5hrs
- The Integrity Check Value (ICV) algorithm is not appropriate
  - The WEP ICV is based on CRC-32, a good error-detection algorithm, but an awful choice for a cryptographic hash.
- RC4 is not good
  - Relatively strong correlation between key and output
- Authentication easily forged

Breaking WEP

Security hole:

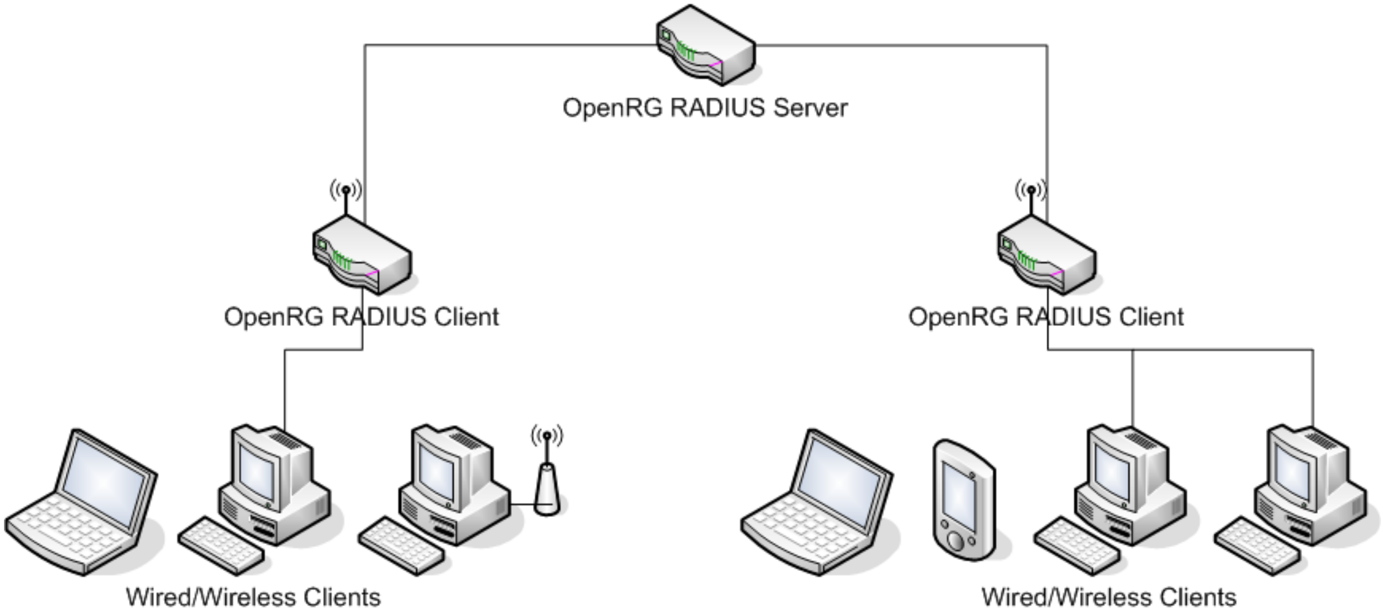
- 24-bit IV, one IV per frame, -> IV's eventually reused
- IV transmitted in plaintext -> IV reuse detected

Attack:

- Trudy causes Alice to encrypt known plaintext d_1 d_2 d_3 d_4 …
- Trudy sees: $c_i = d_i$ XOR k_i^{IV}
- Trudy knows c_i d_i, so can compute k_i^{IV}
- Trudy knows encrypting key sequence k_1^{IV} k_2^{IV} k_3^{IV} …
- Next time IV is used, Trudy can decrypt!

Slightly Better Authentication: 802.1x

- 802.1x (EAP, LEAP, PEAP)
  - All wireless traffic is encrypted
  - Each user can be assigned a unique user name and password, usually to authenticate to a RADIUS server
  - Each user uses a different WEP Key
  - Each user's session uses a different WEP Key



Wi-Fi Protected Access (WPA)

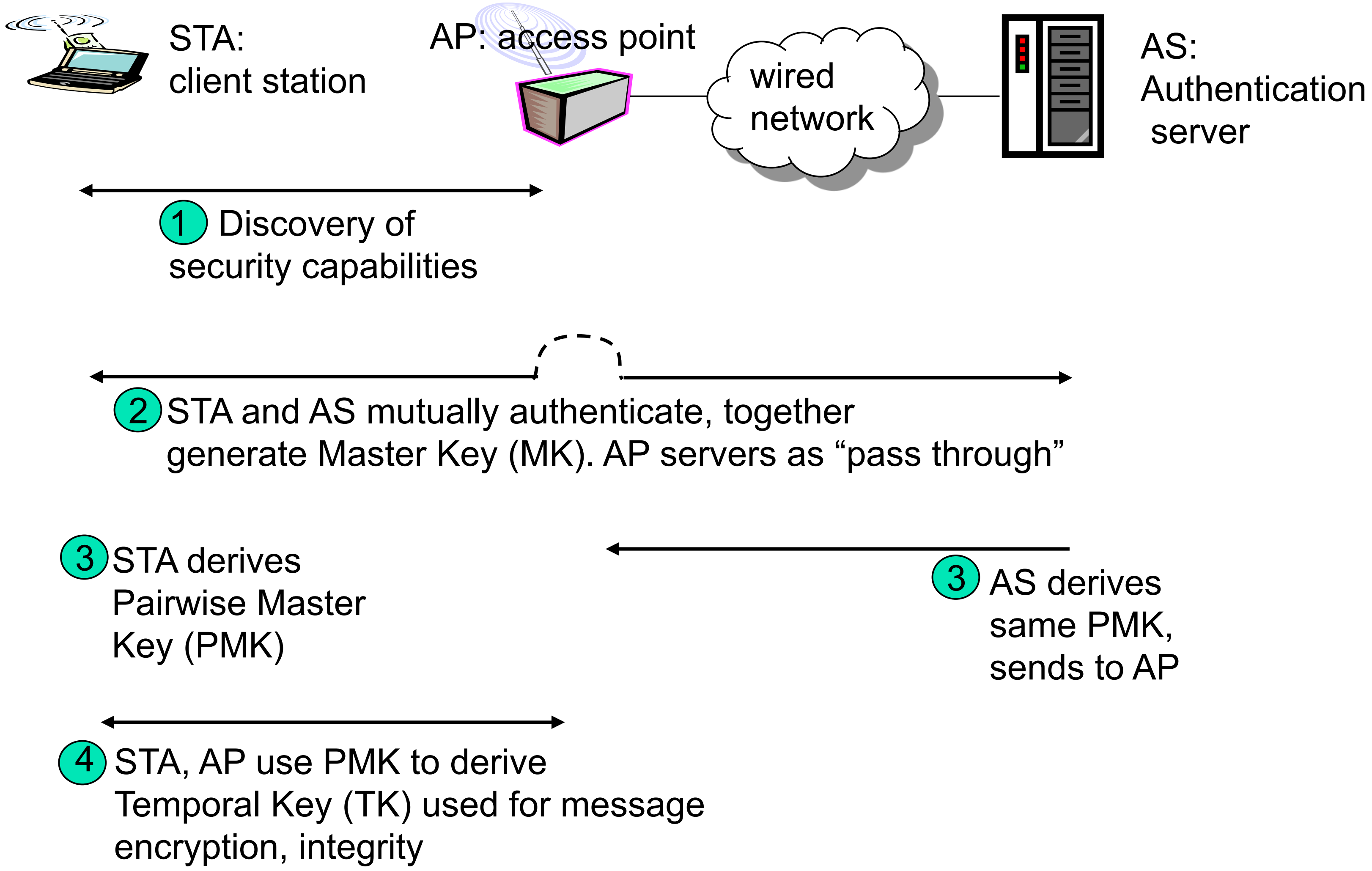
- WPA is a security guideline issued by the Wi-Fi Alliance.
- Goal: strengthen security over WEP with only firmware/ software updates, not hardware updates
- Path: WEP -> WPA -> 802.11i = WPA2
- WPA = TKIP (Temporal Key Integrity Protocol) + IEEE 802.1x
  - *For encryption*: WPA uses TKIP, which uses the same encryption algorithm as WEP, but constructs keys in a different way.
  - *For authentication*: WPA use IEEE 802.1x
- 2 modes:
  - WPA Enterprise : TKIP/MIC ; 802.1X/EAP
  - WPA Personal : TKIP/MIC ; PSK

WPA2 = 802.11i

- Requires hardware updates
- Requires authentication of control packets
- Backward compatible with WPA

- Basically
  - WPA2 = 802.11i = TKIP + IEEE 802.1x + ***AES***

802.11i: four phases of operation



1 Discovery of security capabilities

2 STA and AS mutually authenticate, together generate Master Key (MK). AP servers as “pass through”

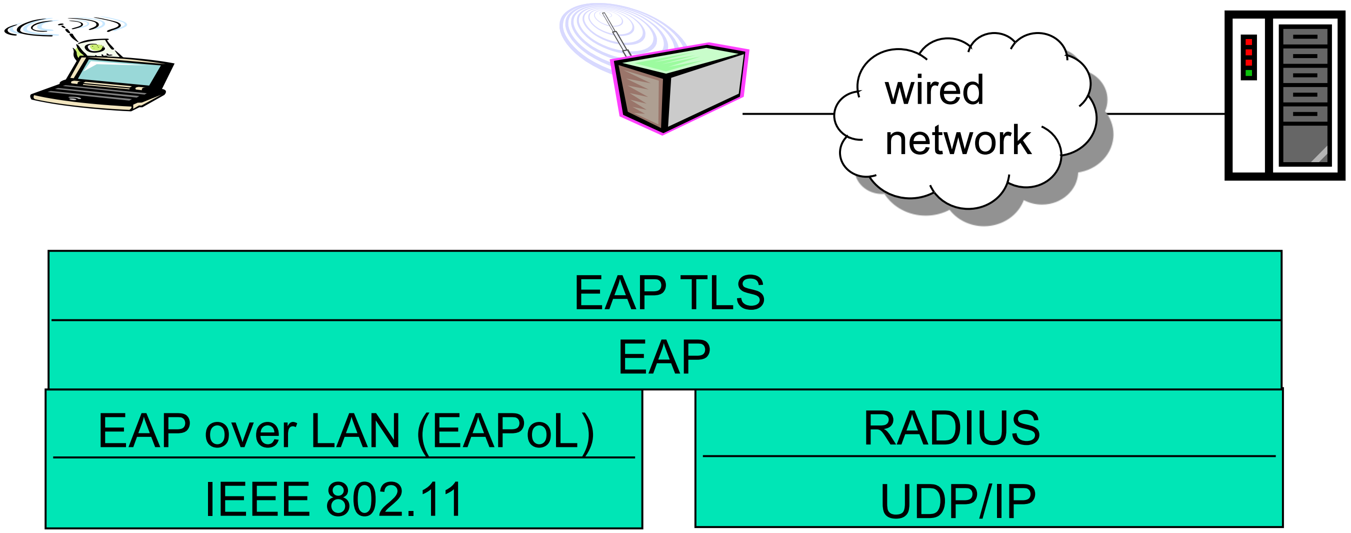
3 STA derives Pairwise Master Key (PMK)

3 AS derives same PMK, sends to AP

4 STA, AP use PMK to derive Temporal Key (TK) used for message encryption, integrity

EAP: extensible authentication protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate "links"
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)



EAP TLS

EAP

EAP over LAN (EAPoL) | RADIUS

IEEE 802.11 | UDP/IP

Summary: “Secure” a WLAN

- Change default ‘admin’ password for wireless router
  - No body is hacking that ☺
- Enable MAC Filtering
  - But MAC sent in clear text! Hassle to maintain
- SSID “Hiding”
  - Change default SSID, choose “*don’t broadcast SSID*”
    - Some wireless router doesn’t support this
  - SSIDs are transmitted in clear text anyhow
- *Use WPA2 + EAS if possible!*