Wireless and Mobile Security

Includes few slides from J.F Kurose and K.W. Ross, “Computer Networking: A Top-Down Approach, 8th edition, Pearson, 2020

University of Minho, 2025, pmc

Outline

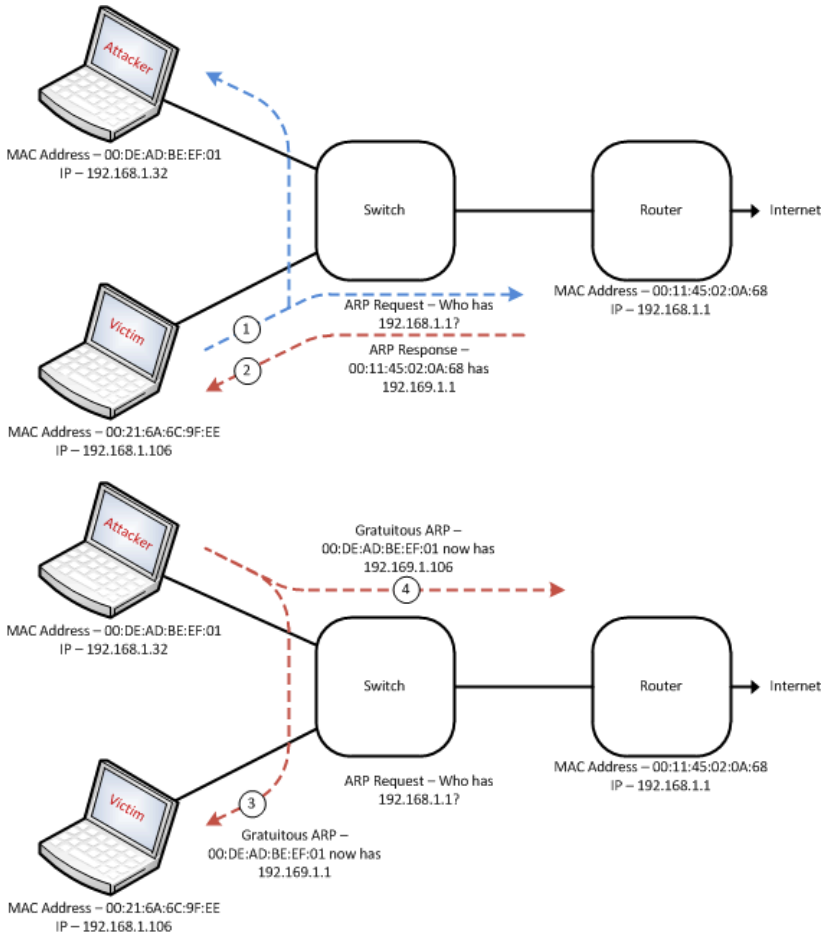
- Security at Link Layer
  - Spoofing
  - IEEE 802.1X
  - VLANs
  - SPTs
- Security in wireless networks
  - Wireless Security Protocols
  - IEEE 802.11 (Wi-Fi)
  - IEEE 802.15.1 (Bluetooth)
  - IEEE 802.15.4 (LP-WPAN)
- Security in mobile networks
  - Cellular networks 4G/5G

Security at Link Layer

- MAC spoofing
  - attacker changes the Media Access Control (MAC) address of its device to impersonate a legitimate device on the network
    - MAC addresses are highly vulnerable, easily changeable in software
  - Potential attacks – bypass access controls or intercept traffic meant for the original device, leading to potential data interception (MitM) or DoS (by flooding the LAN or blackholing)
  - Mitigation
    - Dynamic ARP Inspection (DAI) – validates ARP packets in the network and helps preventing MAC spoofing by verifying a DB of IP-MAC bindings
    - MACsec (802.1AE) – encrypts and authenticates Ethernet frames, providing a robust layer of protection against MAC spoofing

Security at Link Layer

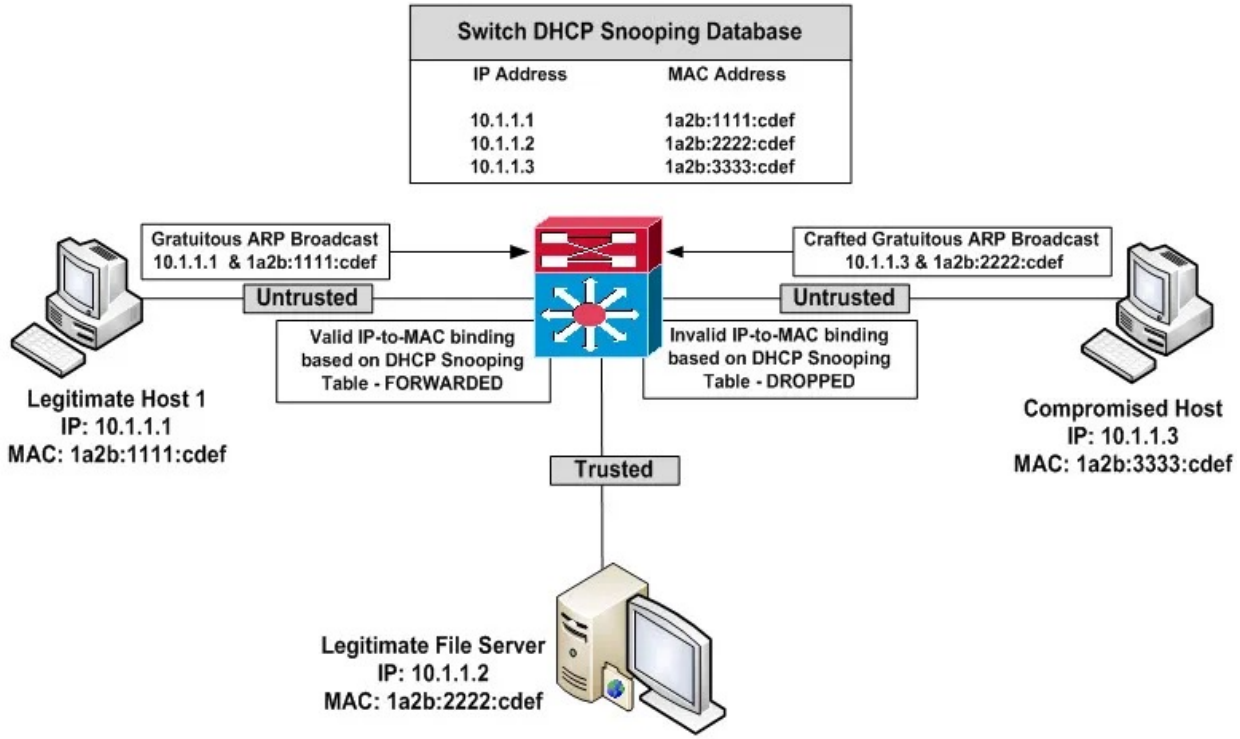
- ARP spoofing (aka ARP Poisoning)
  - prevalent attack at LL, used to intercept / manipulate traffic in LAN
  - attacker sends malicious ARP messages to associate its MAC address with the IP address of another device (e.g., router or legitimate client) to intercept traffic intended for the targeted device
  - fake ARP replies may cause ARP cache poisoning with the attacker's MAC address for a particular IP address (MitM or DoS)



Security at Link Layer

- Mitigation Techniques for ARP Spoofing
  - Static ARP Entries
    - solves but difficult to manage in large, dynamic networks
  - Dynamic ARP Inspection (DAI)
    - validates ARP requests/replies against a trusted DB (e.g., DHCP snooping bindings)
    - requires compatible network hardware and proper configuration to be effective
  - LAN segmentation
    - segmenting the network into VLANs isolates sensitive devices, making it more difficult for an attacker to conduct ARP spoofing across different segments
    - reduces the attack surface
    - requires VLAN-capable hardware and careful network planning
  - Monitoring / detection tools
    - e.g., *arpwatch*, *XArp*, and IDSs help in detecting suspicious ARP activity in RT

Security at Link Layer



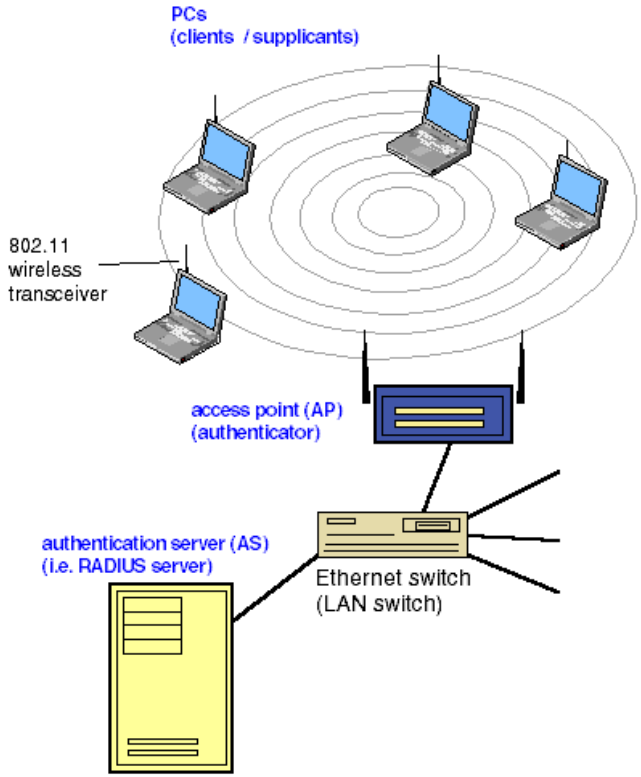
- Example of Dynamic ARP Inspection with DHCP snooping bindings

Security at Link Layer

- Port security mechanisms
  - essential for ensuring that only authorized devices can connect to LANs/WLANs
  - MAC address filtering
    - network admin defines a list of allowed MAC addresses
    - useful in small networks, challenging to scale
  - Limiting #MAC addresses per port
    - shutdown port or blocking new addresses if limit exceeded
  - MACsec (IEEE 802.1AE)
    - provides frame-by-frame encryption and authentication
    - provides a robust layer of data confidentiality and integrity in Ethernet LANs
    - often deployed between critical network components (switches) and endpoint devices in sensitive, high-security environments (e.g., government and finance)
  - IEEE 802.1X authentication (with RADIUS)

802.1X Authentication and Network Access Control

- IEEE 802.1X
  - auth and network access control standard widely used to secure LANs, particularly in enterprise and educational environments
  - it ensures that only authenticated users and devices can access the network by enforcing security at the "port" level (e.g., Ethernet port or AP)
  - part of IEEE 802 standards, adds an extra security layer to LANs

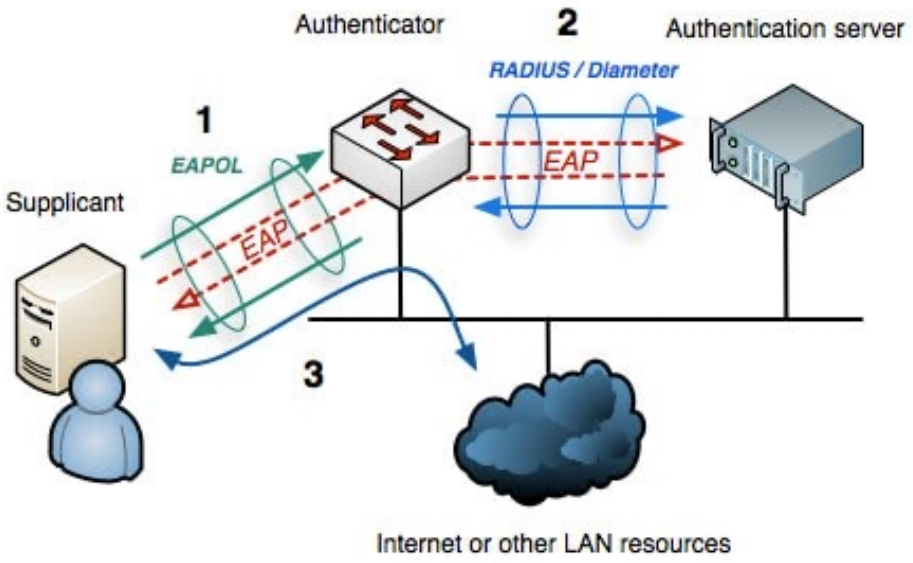


802.1X Authentication and Network Access Control

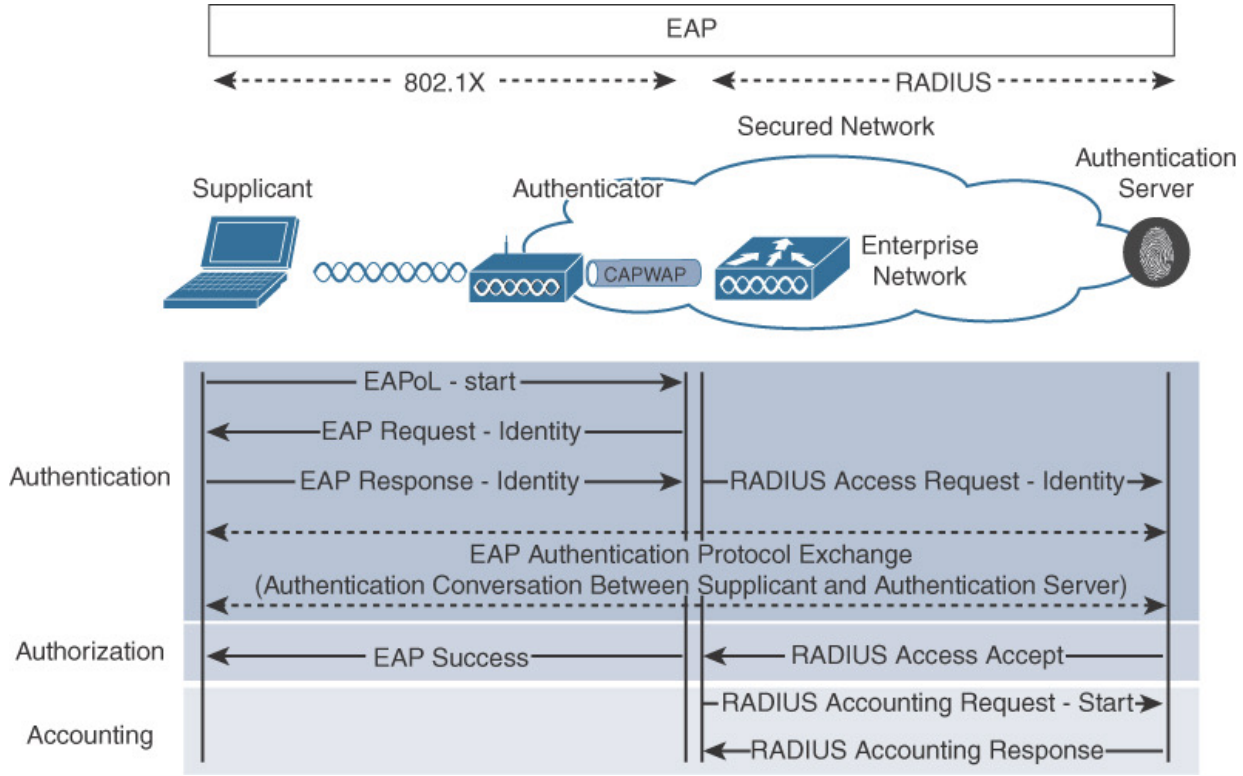
- 802.1X Key Components
  - Supplicant – client device seeking network access (e.g., laptop, smartphone)
  - Authenticator – network device that controls access, such as a switch or access point
    - the authenticator forwards authentication requests to the authentication server and acts as a gatekeeper/proxy, blocking or allowing access based on authentication outcome
  - Authentication Server – usually a RADIUS (Remote Authentication Dial-In User Service) server that validates credentials
    - verifies whether the user or device should be granted network access

802.1X Authentication and Network Access Control

- 802.1X Authentication Process
  1. Initiation – the supplicant requests network access to Authenticator (switch or AP) using EAP (Extensible Authentication Protocol) over LAN exchange
  2. Authentication Server Verification using EAP over Radius / Diameter
  3. Access Granted (or denied)



802.1X Authentication and Network Access Control



- 802.1X Authentication Process RADIUS (Remote Authentication Dial-In User Service)

802.1X Authentication and Network Access Control

- Common 802.1X EAP Methods
  - Lightweight EAP (LEAP) – client simply provides to AS its credentials (username and password); highly insecure, deprecated since 2003
  - Protected EAP (PEAP) – uses inner and outer authentication
    - sets an encrypted TLS tunnel between client and AS using only a server-side certificate
    - then uses username and password credentials already in org identity store
    - the most widely deployed method (e.g., Microsoft Active Directory)
  - EAP-TLS – mutual, certificate-based authentication method
    - requires a digital certificate on both AS server and the client device
    - a TLS tunnel is built to exchange encryption keys, no passwords involved
    - the most secure, more complex to implement and manage

802.1X Authentication and Network Access Control

- 802.1X Summary
  - Enhanced Security – 802.1X prevents unauthorized users from accessing the network and provides an additional layer of control, particularly valuable for managing access in larger networks
  - Flexibility with EAP – EAP supports various methods (e.g., LEAP, EAP-FAST, PEAP, EAP-TTLS, EAP-TLS), administrators can select the method that best balances security and user capabilities
  - Integration with RADIUS – 802.1X typically relies on RADIUS servers, which also offer accounting and auditing features for tracking and analysing access patterns and security threats

Although 802.1X is robust and secure, does any security concern remain?

802.1X Authentication and Network Access Control

- yes, mainly due to improper implementation, use of weaker authentication methods, or vulnerabilities in dependent systems

  concerns:
  - weak EAP methods, i.e., without mutual authentication
  - "evil twin" or rogue AP/switch to capture user credentials
  - EAP and RADIUS misconfigurations
  - scalability and certificate management in large networks
- Best practices
  - use mutual authentication (EAP-TLS, if possible); MACsec (802.1AE); enforce strong password policies and certificate management; regular network monitoring and auditing

Outline

- Security at Link Layer
  - Spoofing
  - IEEE 802.1X
  - VLANs
  - SPTs
- Security in wireless networks
  - Wireless Security Protocols
  - IEEE 802.11 (Wi-Fi)
  - IEEE 802.15.1 (Bluetooth)
  - IEEE 802.15.4 (LP-WPAN)
- Security in mobile networks
  - Cellular networks 4G/5G

WLANs Security

Goals:

- Identify different types of wireless network attacks
- List vulnerabilities of WLAN security
- Understand WLAN security mechanisms and components
- Plan solutions for securing wireless networks

- Two important (but different) challenges:
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network

WLANs Security

Facts:

- Conversely to wired LAN, WLANs don't have a single entry-point
  - attacker can be anywhere within the LAN coverage area, even outside premises
- Wireless RF signal is usually omnidirectional, eavesdropping data communications is trivial
- Misconfigured Access Points may allow an intruder to get in the LAN or install malware

WLANs Type of Attacks

1- Rouge Access Point

- unauthorized, untrusted AP connected to the network infrastructure bypassing enterprise, institution or organization security policies
- may work as a network entry point for attacker as it circumvents established network security procedures and configurations
- does not need to be a separate network device, WNICs can be virtualized
- internal risk (e.g., employee, student)

Rouge or misconfigured APs may allow access to network intruders
behind firewall

WLANs Type of Attacks

2- Evil Twin

- AP set by an attacker designed to mimic an authorized AP with objective to deceive users' association, and capture transactions

3- Intercepting WLAN Traffic

- eavesdropping RF signal

4- WLAN DoS

- RF signal interference; radio spectrum flooding (jamming)
- spoofing management frames from STA to AP (disassociation attack)
- attacker may manipulate “duration”* of RTS frame (taken by transmission + ACK) to an arbitrary high value impairing other STAs from transmission

*max value = 32.7 ms

WLANs Type of Attacks

If successful, attackers may…

Steal data

- as consequence of poorly configured security

Read transmissions

- attacker may access to sensitive data

Inject malware

- as attacker is behind the firewall, may inject malware, viruses, etc.

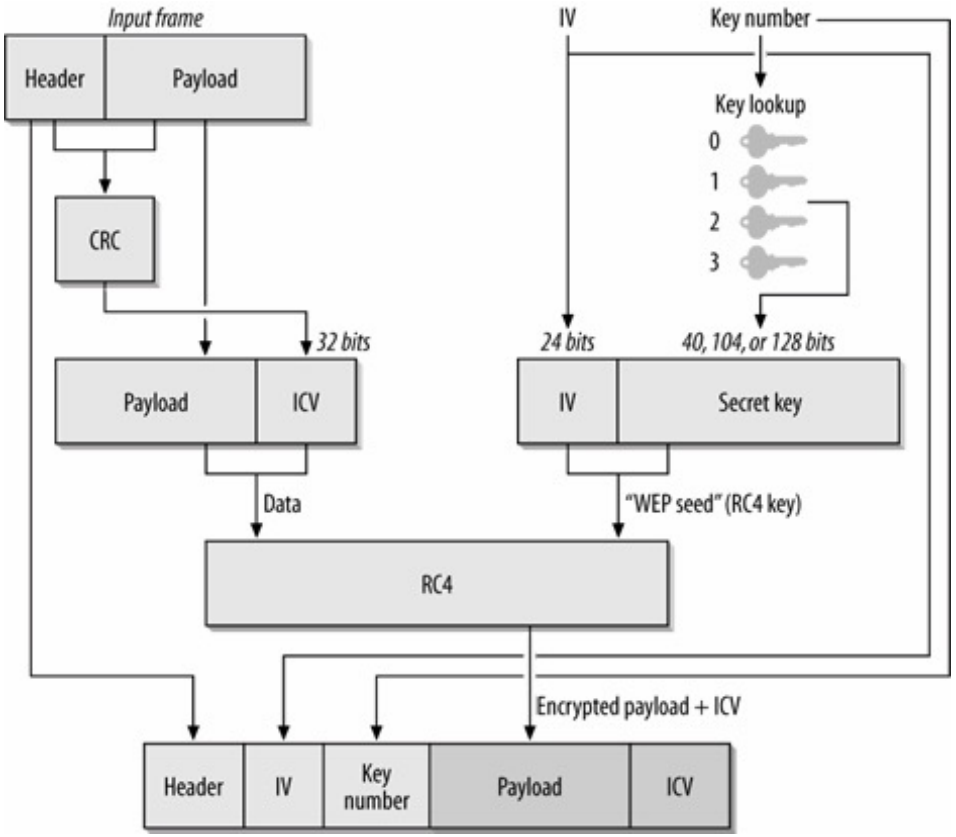
Harmful contents

- attacker may download and distribute harmful contents from an unprotected STA in the WLAN

Wireless Security Protocols

Wired Equivalent Privacy (WEP)

- part of the original IEEE 802.11 standard (1997) to encrypted WLAN communications
- STAs and AP use a shared key combined with an Initialization Vector (IV) (64 bits minimum), which works as WEP seed
- an RC4 key is generated, each time a frame is sent
- encryption uses stream cypher algorithm RC4 (Rivest Cypher 4)



Wireless Security Protocols

WEP

- provides weak encryption; vulnerable RC4 stream cipher
- short IV cycles fast (each 2^{24} values; few hours in a 54Mbps WLAN) generating detectable patterns used by attackers to crack encryption
- 64- or 128-bit static key; easily cracked (e.g., aircrack-ng)
- unsecure; Wi-Fi Alliance deprecated WEP in 2004

Wi-Fi Protected Setup (WPS)

- simple; relies on a PIN to setup security configuration between wireless router/AP and STA; commonly used by wireless printers
- PIN is divided in two halves (4,3 bits) and last bit used for checksum; easy to crack using brute force
- WPS is recommended to be disabled in wireless routers

Wireless Security Protocols

Wi-Fi Protected Access (WPA)

- Wi-Fi Alliance proposal (2004) as an improvement of WEP
- implements TKIP (Temporal Key Integrity Protocol) to dynamically change keys and prevent key reuse
  - Pairwise Transient Key: $\mathtt{PTK} = \mathtt{KDF}\,(\mathtt{PMK}^{*}, \mathtt{Anonce}, \mathtt{Snonce}, \mathtt{MAC}_{\mathtt{AP}}, \mathtt{MAC}_{\mathtt{STA}})$
- WPA Personal (SOHO, up to ten users)
  - uses open mode or pre-shared key (PSK) (secret key similarly to WEP)
  - authorized STAs with PSK authenticate automatically with AP
- WPA Enterprise
  - allows access control per STA in a centralized way (IEEE 802.1X + RADIUS AS)
- more secure than WEP but still relies on RC4 for compatibility
- WPA's TKIP encryption is also outdated and vulnerable to attacks

*PMK – Pairwise Master Key is derived from (PSK, SSID).

Wireless Security Protocols

- WPA (Wi-Fi Protected Access) Vulnerabilities
  - techniques such as key reinstallation attacks (KRACK), packet injection and replay attacks can exploit weaknesses in WEP and WPA

Vulnerability Type	Description	Mitigation/Resolution
TKIP Weaknesses	Weak RC4 encryption, Michael algorithm for integrity checks flaws	Use WPA2 with AES-CCMP
Brute-Force on PSK	Password-guessing of shared keys	Use complex passphrases
KRACK Attack	Forces key reinstallation during handshaking, leading to traffic decryption	Use WPA3
Packet Injection	Exploits weaknesses in message integrity	Use WPA2 with AES-CCMP or WPA3
Replay Attacks	Reuse of captured packets disrupts communications	Use WPA2 with AES-CCMP

Wireless Security Protocols

- WPA2
  - replaces WPA's TKIP with more secure Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
    - uses CBC-MAC for integrity, CBC-MAC based on AES for encryption
  - Personal PSK mode
    - can be vulnerable to BF attacks if weak passwords are used
  - Enterprise mode
    - uses 802.1X auth with RADIUS server, using individual auth credentials
  - still suffers WPA vulnerabilities for specific WPA2 configurations (in TKIP, GCMP cipher implementations in WPA2 for backward compatibility)
  - Wi-Fi Alliance deprecated TKIP in 2012 and strongly recommends using WPA2 with AES-CCMP only, or upgrading to WPA3

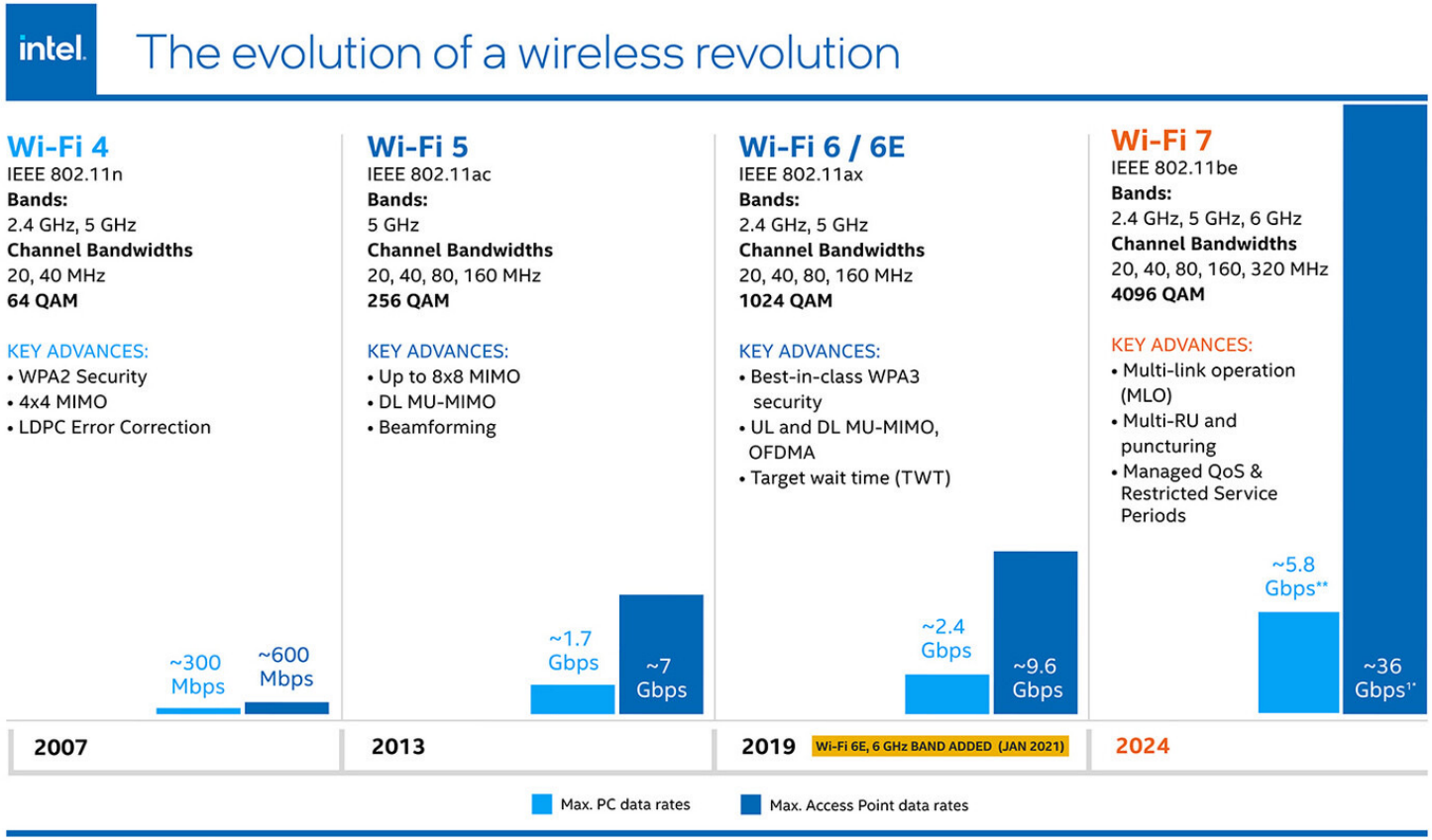
Wireless Security Protocols

- WPA3
  - enhances security over WPA2 by requiring SAE (Simultaneous Authentication of Equals) for key exchange in Personal mode, protecting against BF attacks
    - replaces PSK authentication method used in WPA2 to avoid offline dictionary attacks; capturing the handshaking is no longer enough
    - PMK is generated dynamically for each connection using a combination of password and random values, based on Elliptic Curve Cryptography, instead of password and SSID (WPA2)
    - forward secrecy
  - better encryption for open WLANs through Opportunistic Wireless Encryption (OWE) (Wi-Fi Alliance, 2018) [RFC 8110]
    - e.g., for use in public, open hotspots

Wireless Security Protocols

Protocol	Encryption	Integrity	Authentication	Key Management	Main Vulnerabilities	Comments
WEP	RC4	CRC-32	Shared Key (PSK)	Static keys	Weak IV reuse, RC4 vulnerabilities	Outdated, highly vulnerable
					Susceptible to packet injection	No longer secure or recommended
WPA	RC4 (with TKIP)	Michael algorithm	PSK or 802.1X (Enterprise)	Temporal Key Integrity Protocol	TKIP weaknesses, brute-force on PSK	Interim solution to improve WEP
					Vulnerable to KRACK attack	PSK still weak; phased out for WPA2
WPA2	AES-CCMP	CCMP (based on AES)	PSK or 802.1X (Enterprise)	AES key exchange with CCMP	KRACK attack on WPA2	Industry standard for secure Wi-Fi
					Vulnerable to PSK brute-force	WPA2-Enterprise more secure
WPA3	AES-CCMP (Personal & Enterprise)	HMAC and PMF for integrity	SAE (Personal) or 802.1X (Enterprise)	Protected Management Frames (PMF)	Relatively secure; mitigates KRACK	Latest and most secure protocol
	AES-GCMP (Enterprise-192)			Forward secrecy, OWE for open Wi-Fi	Reduces risks of brute-force attacks	Mandatory for new devices (2020)

Recent WLANs Standards

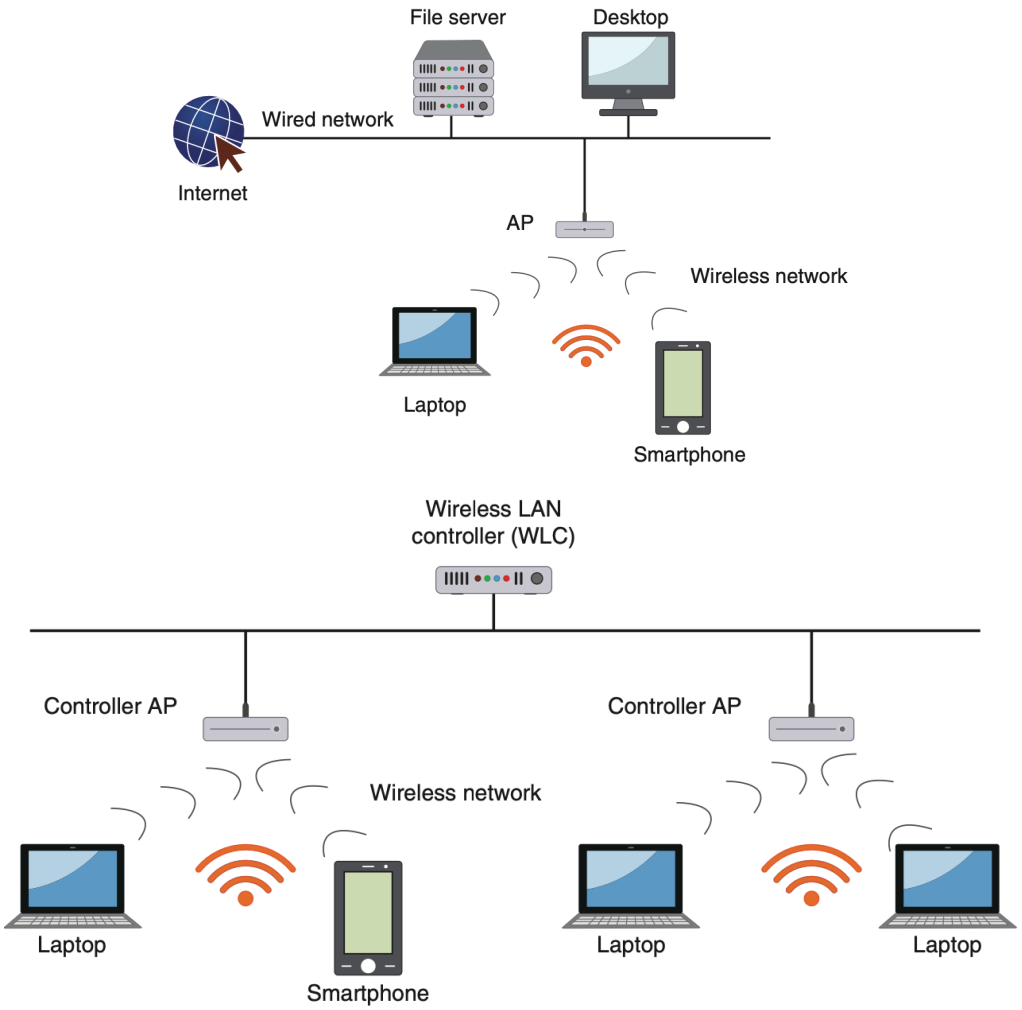


1 Includes PHY and multi-link data rate improvements
* Theoretical maximum data rates based on the latest draft of the IEEE 802.11be standard.
** ">5 Gbps Wi-Fi 7 2x2 client speed" - is based on the current draft of the 802.11be specification which specifies the theoretical maximum data rate for a 2x2 device that supports 320 MHz channels, 4096 QAM, and Multi-Link Operation is 5.76 Gbps. Based on an industry-standard assumption of 90% efficiency for new Wi-Fi products operating in the exclusive 6 GHz band, the resulting estimated maximum over the air 2x2 client speed would be 5.19 Gbps.

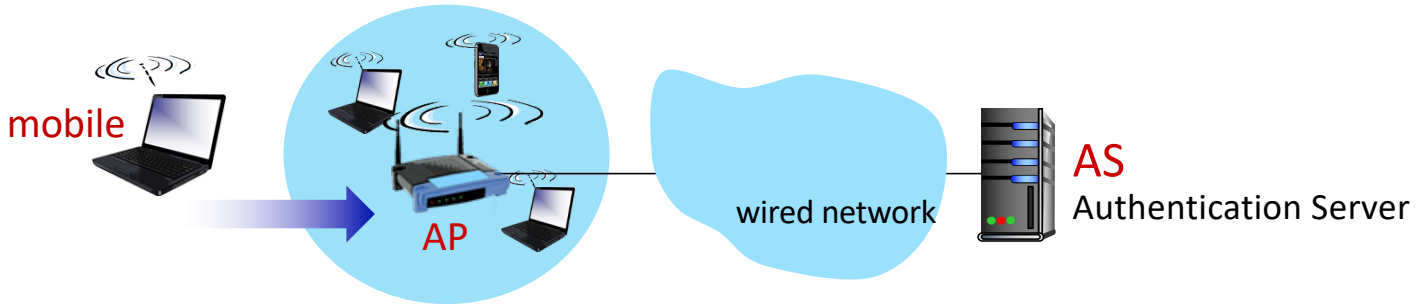
WLANs Access

Infrastructure mode (via AP)

- Fat vs. Thin Access Point (AP)
  - autonomous device including wireless management functions, authentication, encryption, etc. vs. simpler device w/ many management functions centered on WLAN switch.
- Controller AP
  - improves thin APs performance thru a Wireless LAN Controller (WLC)
- Captive Portal AP
  - common public hotspots from ISP; interacts with user via web browser



Security in WLANs 802.11



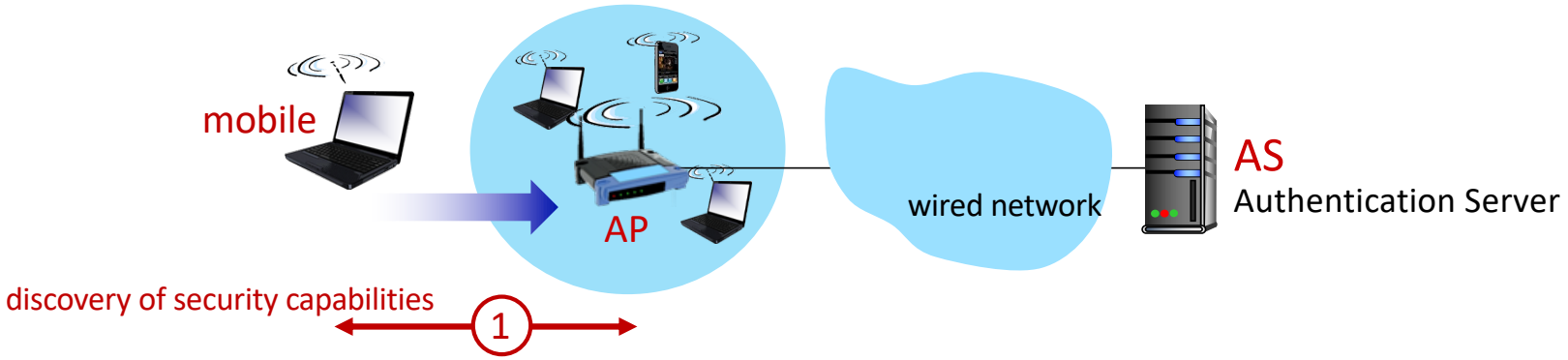
Arriving mobile must:

- authenticate and associate with access point (AP): establish communication over wireless link
- may need to authenticate to network

Security in WLANs 802.11

- When a user joins a Wi-Fi network, the 802.1X process, if present, is embedded in the 802.11 association phase
- Steps:
  1. 802.11 Authentication and Association
  2. 802.1X/EAP Authentication
     - after association, AP acts as the Authenticator in the 802.1X framework
     - used in enterprise Wi-Fi networks (not in home Wi-Fi networks)
  3. Data Encryption with WPA/WPA2/WPA3
     - WPA-Personal mode (based on a shared password) is commonly used for smaller, less complex setups without a RADIUS server
     - WPA-Enterprise mode, which uses 802.1X, is generally the choice for secure, enterprise-level networks

Security in WLANs 802.11

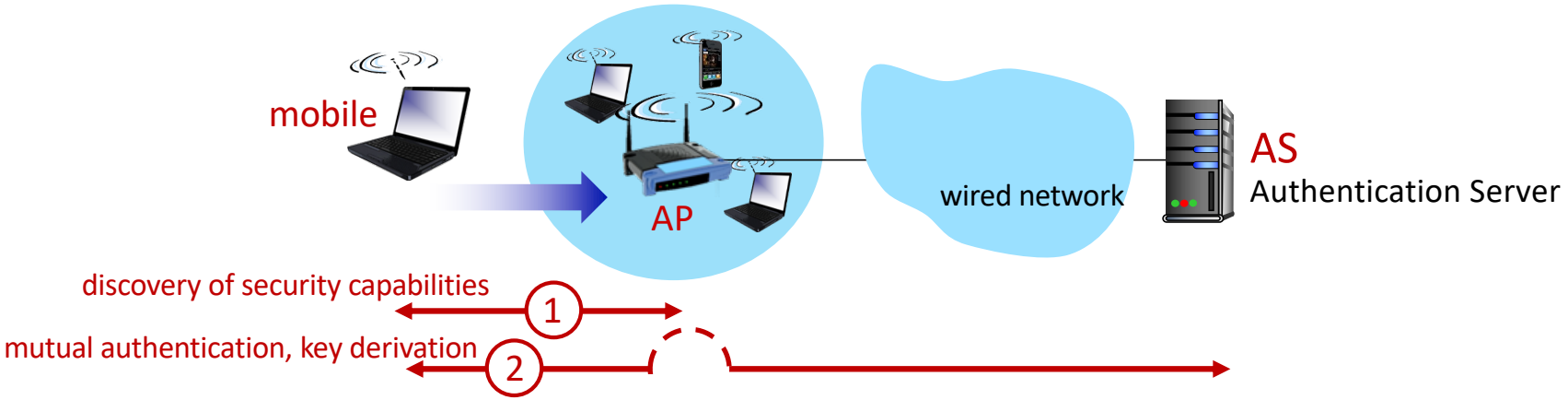


1 discovery of security capabilities:

- AP advertises its presence, forms of authentication and encryption provided
  - e.g., 802.1X AKM (Authentication and Key Management) using SHA-256 or SHA-384
- device requests specific form of authentication, encryption desired

although device, AP already exchanging messages, device not yet authenticated, does not have encryption keys (pre-association phase)

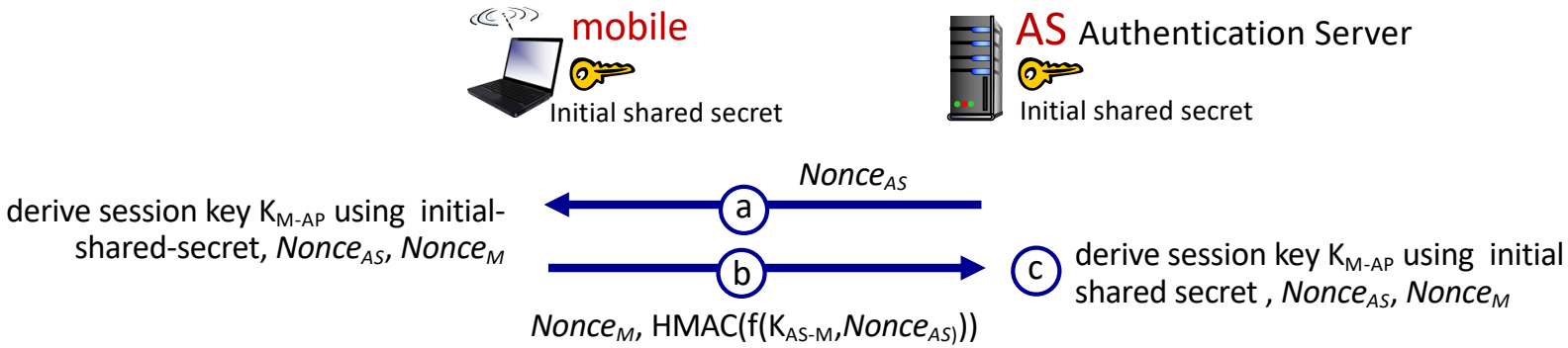
Security in WLANs 802.11



② mutual authentication and shared symmetric key derivation:

- AS, mobile already have shared common secret (e.g., password)
- AS, mobile use shared secret, nonces (prevent relay attacks), cryptographic hashing (ensure message integrity) to authenticate each other
- AS, mobile derive symmetric session key (PKM - Pairwise Master Key)

Security in WLANs 802.11: WPA3 handshake



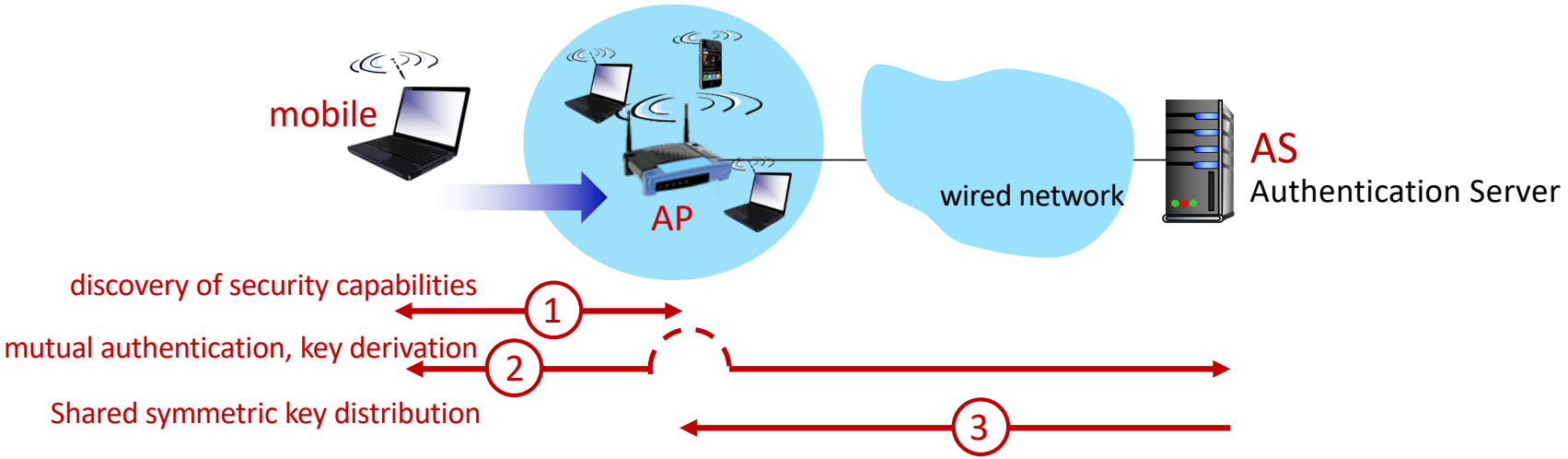
ⓐ AS generates $Nonce_{AS}$, sends to mobile

ⓑ mobile receives $Nonce_{AS}$

- generates $Nonce_M$
- generates symmetric shared session key K_{M-AP} using initial shared secret, $Nonce_{AS}$, and $Nonce_M$
- sends $Nonce_M$, and HMAC-signed value of $Nonce_{AS}$ and derived session key

ⓒ AS derives symmetric shared session key K_{M-AP}

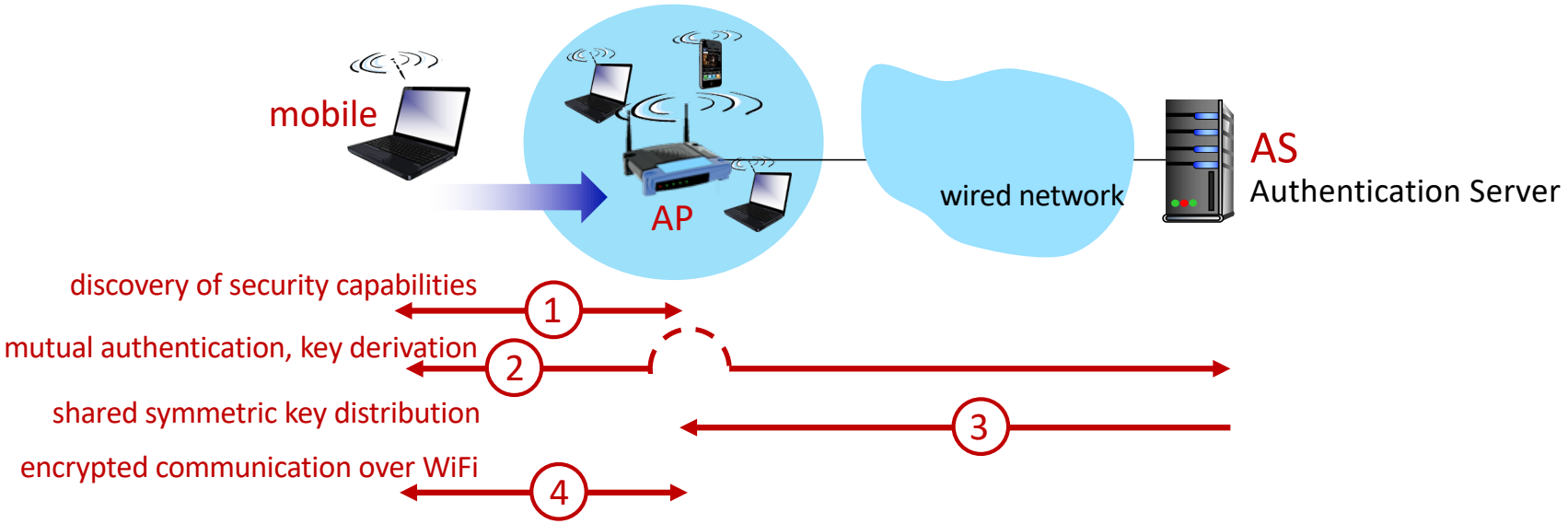
Security in WLANs 802.11



3 shared symmetric session key distribution (e.g., for AES encryption)

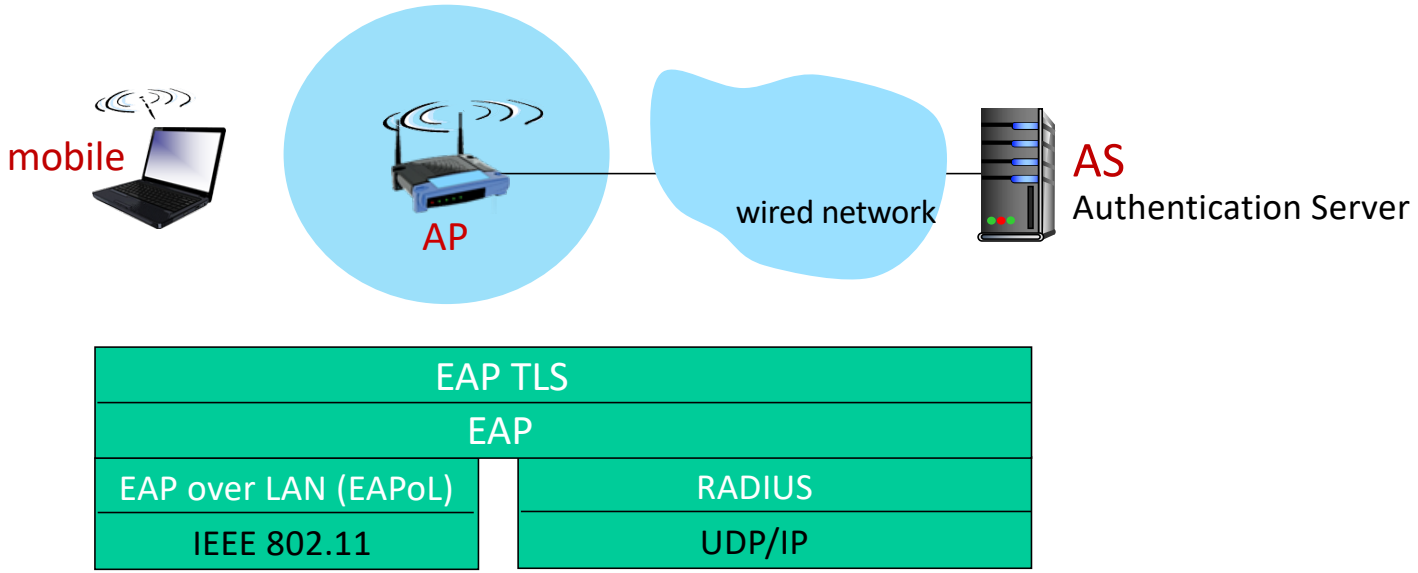
- same key derived at mobile, AS
- AS informs AP of the shared symmetric session

Security in WLANs 802.11



④ encrypted communication between mobile and remote host via AP

Security in WLANs 802.11

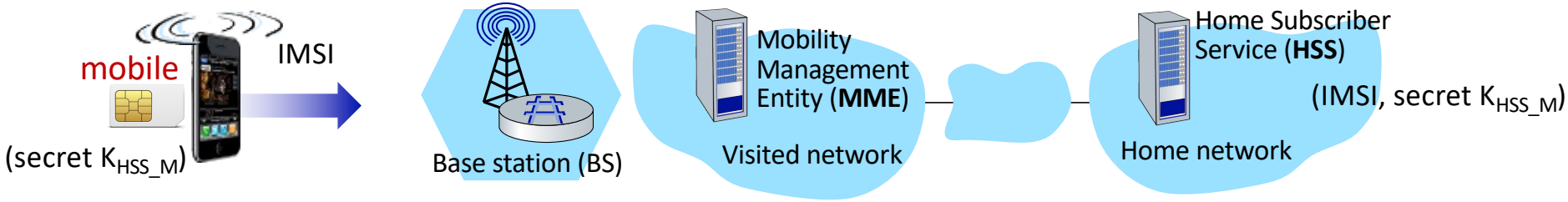


- Extensible Authentication Protocol (EAP) [RFC 3748] defines end-to-end request/response protocol between mobile device, AS

Outline

- Security at Link Layer
  - Spoofing
  - IEEE 802.1X
  - VLANs
  - SPTs
- Security in wireless networks
  - Wireless Security Protocols
  - IEEE 802.11 (Wi-Fi)
  - IEEE 802.15.1 (Bluetooth)
  - IEEE 802.15.4 (LP-WPAN)
- Security in mobile networks
  - Cellular networks 4G/5G (Authentication)

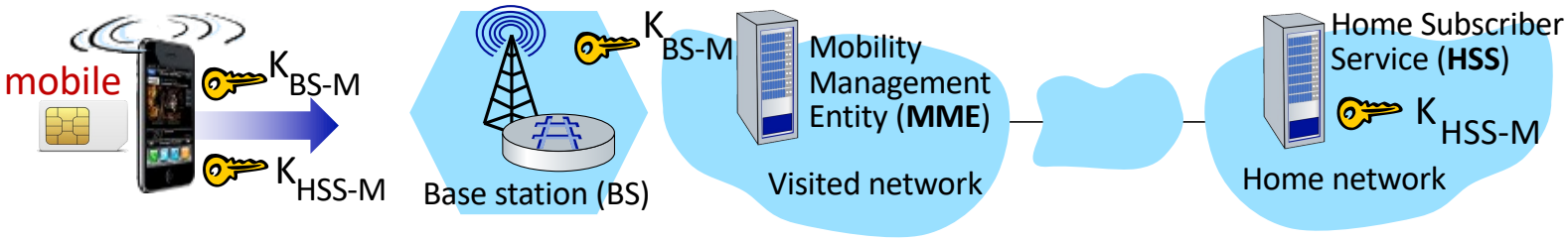
Authentication, encryption in 4G LTE



- arriving mobile must:
  - connect with BS: initial low-level comm over 4G wireless link
  - authenticate itself to network, and authenticate network
- notable differences from WiFi
  - mobile's SIM card provides global identity*, contains shared keys
  - services in visited network depend on (paid) service subscription in home network

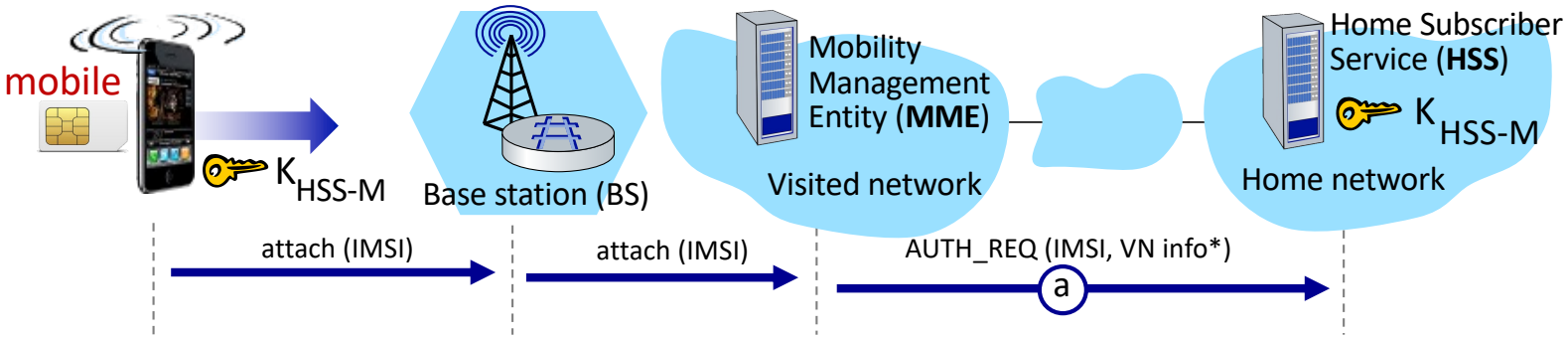
*IMSI – International Mobile Subscriber Identity

Authentication, encryption in 4G LTE



- mobile, BS use derived session key K_{BS-M} to encrypt communications over 4G link
  - all process relies on symmetric key cryptography
- MME in visited network + HSS in home network, together play role of WiFi AS
  - ultimate authenticator is HSS
  - trust and business relationship between visited and home nets

Authentication, encryption in 4G LTE

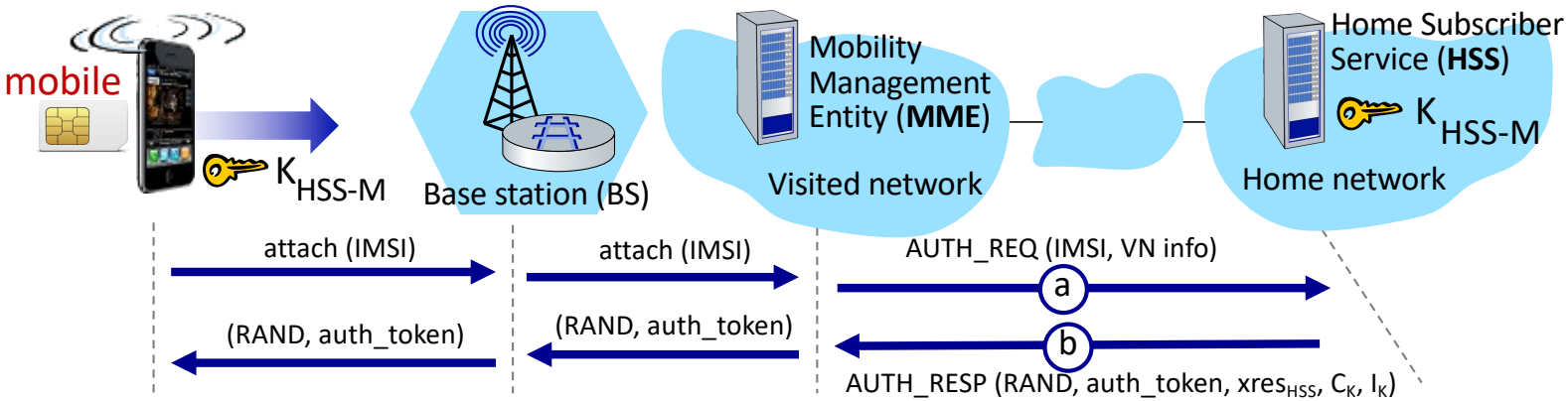


ⓐ authentication request to home network HSS

- mobile sends attach message (containing its IMSI) relayed from BS to visited MME to home HHS
- IMSI identifies mobile's home network

* Visited Network info includes MCC (Mobile Country Code) and MNC (Mobile Network Code)

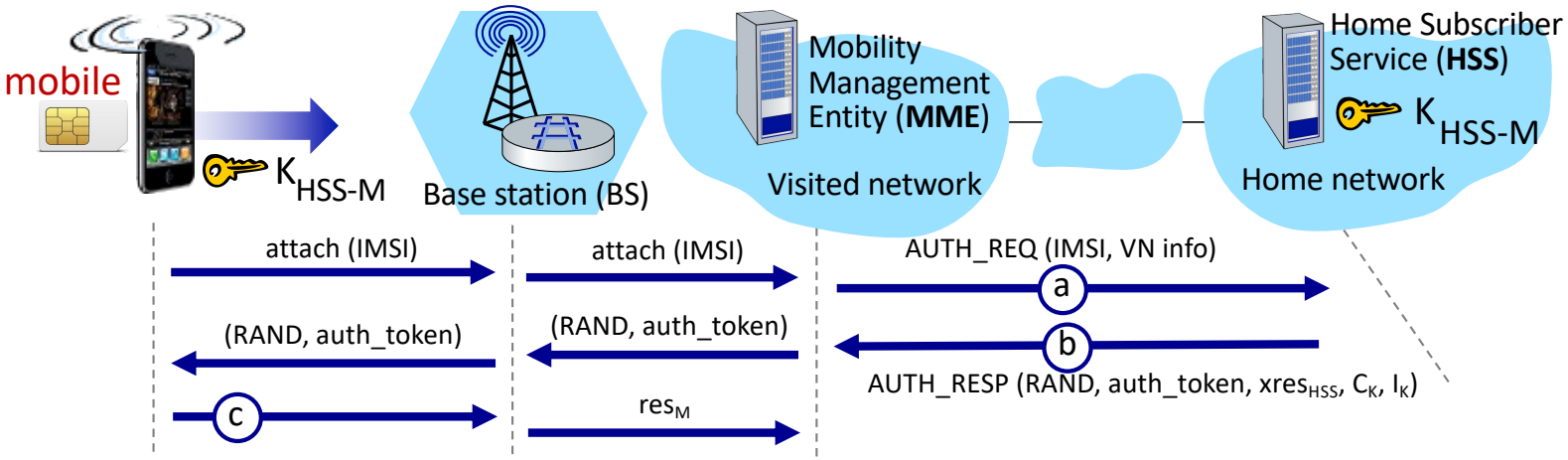
Authentication, encryption in 4G LTE



ⓑ HSS use shared-in-advance secret key, K_{HSS-M}, to derive authentication token, *auth_token*, expected auth response token, $xres_{HSS}$, and base keys

- *auth_token* contains info encrypted by HSS using K_{HSS-M} , allowing mobile to know that whoever computed *auth_token* knows shared-in-advance secret
- mobile has authenticated network
- MME in visited network keeps $xres_{HSS}$, C_K and I_K for later use

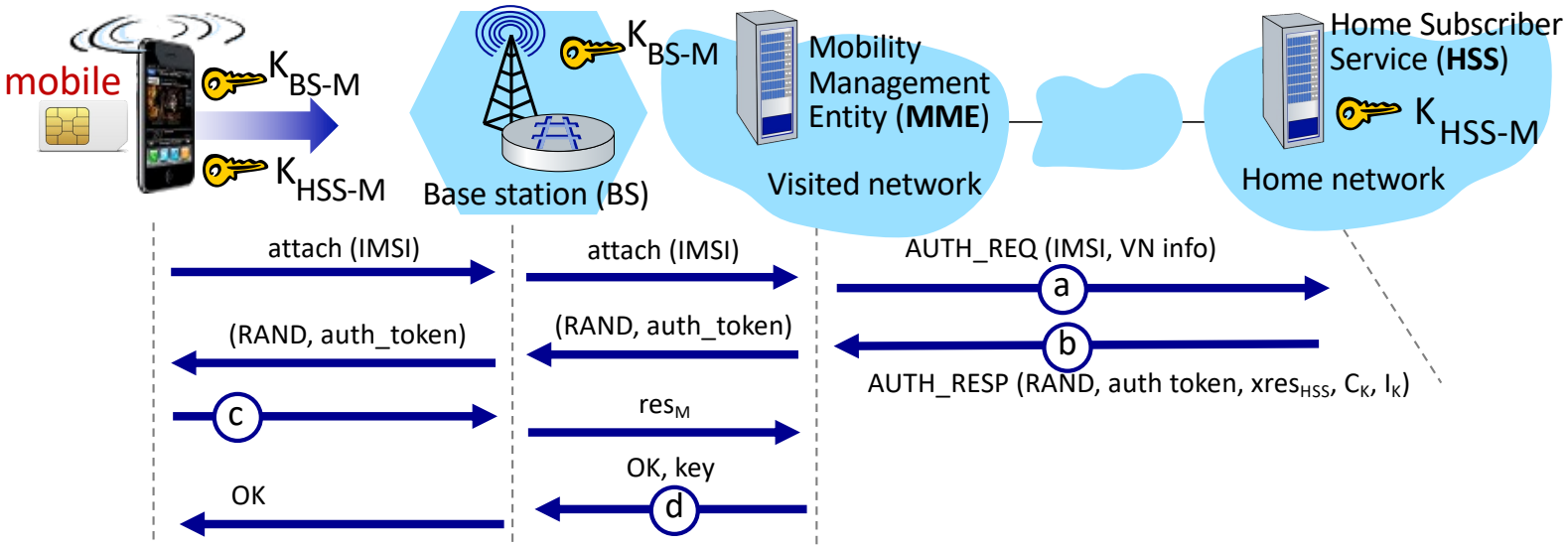
Authentication, encryption in 4G LTE



ⓒ authentication response from mobile:

- mobile computes res_M using its secret key to make same cryptographic calculation that HSS made to compute $xres_{HSS}$, C_K and I_K and sends res_M to MME

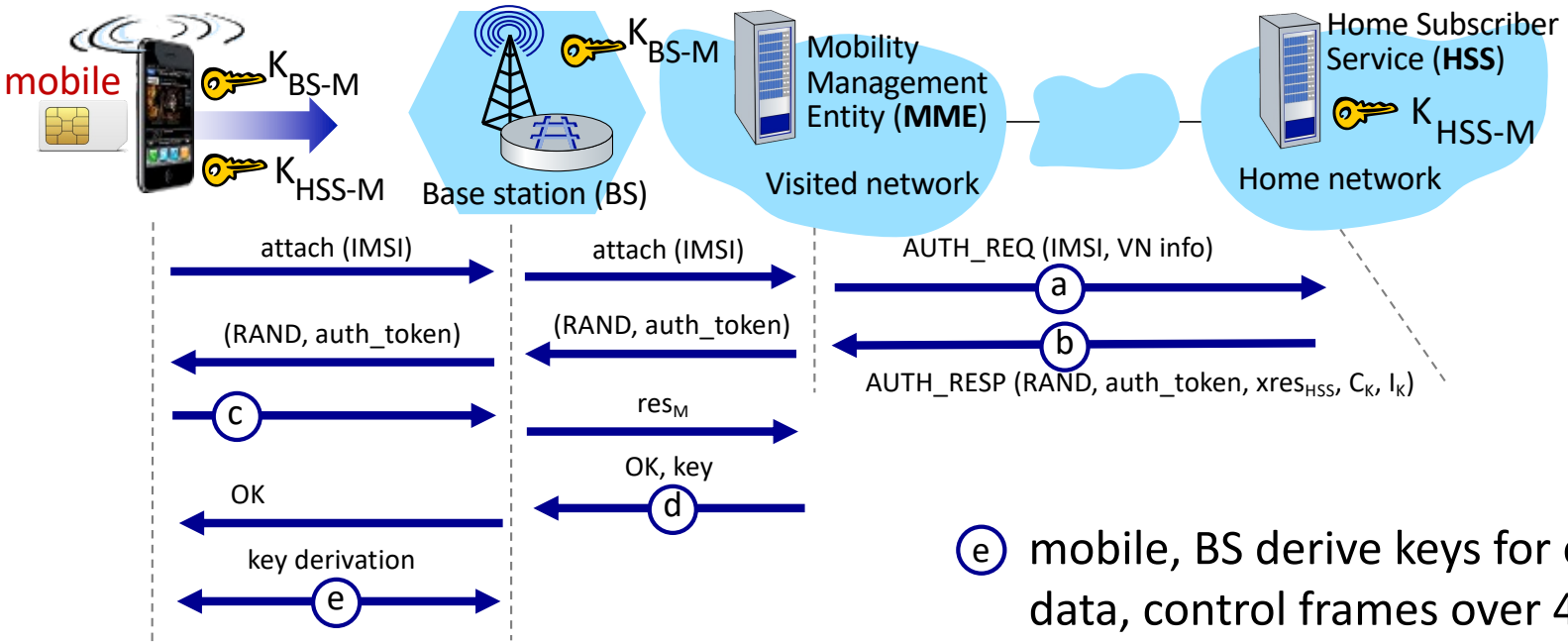
Authentication, encryption in 4G LTE



ⓓ mobile is authenticated by network:

- MME compares mobile-computed value of res_M with the HSS-computed value of $xres_{HSS}$. If they match, mobile is authenticated !
- MME informs BS that mobile is auth; mobile, MME generate master session key K_{BS-M}

Authentication, encryption in 4G LTE



e mobile, BS derive keys for encrypting data, control frames over 4G wireless channel

- AES can be used

Authentication, encryption: from 4G to 5G

- 4G: MME in visited network initiates and manages authentication decision, generates master key ($K_{M\text{-}BS}$)
- 5G: Home network has more control and centralized security management (shift on the key derivation architecture)

- 4G: uses single master (root) key
- 5G: introduces a more complex and granular key hierarchy, for protection

- 4G: device IMSI transmitted in cleartext to BS
- 5G: public key crypto used to encrypt IMSI (SUPI*)

*Subscription Permanent Identifier

Wireless and Mobile Security Summary

- Security at Link Layer
  - Spoofing
  - IEEE 802.1X
  - VLANs
  - SPTs
- Security in wireless networks
  - Wireless Security Protocols
  - IEEE 802.11 (Wi-Fi)
  - IEEE 802.15.1 (Bluetooth)
  - IEEE 802.15.4 (LP-WPAN)
- Security in mobile networks
  - Cellular networks 4G/5G