Ipsec, Wireless security, Firewall, and IDS

CE 352, Computer Networks

Salem Al-Agtash

Lecture 26

Recap (to cover)

Cryptography

- Secret key algorithms: DES/AES
- Public key algorithms: RSA
- One-way hash functions and message integrity: MD5, SHA2

End-point authentication, access control, public key infrastructure, digital signature

Securing the Internet

- Application layer security: Securing email
- Transport layer security: Securing TCP connection - TLS
- Network layer security: IPsec and VPN
- Data link layer (wireless) security: Wireless LAN
- Operational security (Firewall, IDS)

Network-layer Security

between two network entities:

sending entity encrypts datagram payload, payload could be:

- TCP or UDP segment, ICMP message, OSPF message ….

all data sent from one entity to another would be hidden:

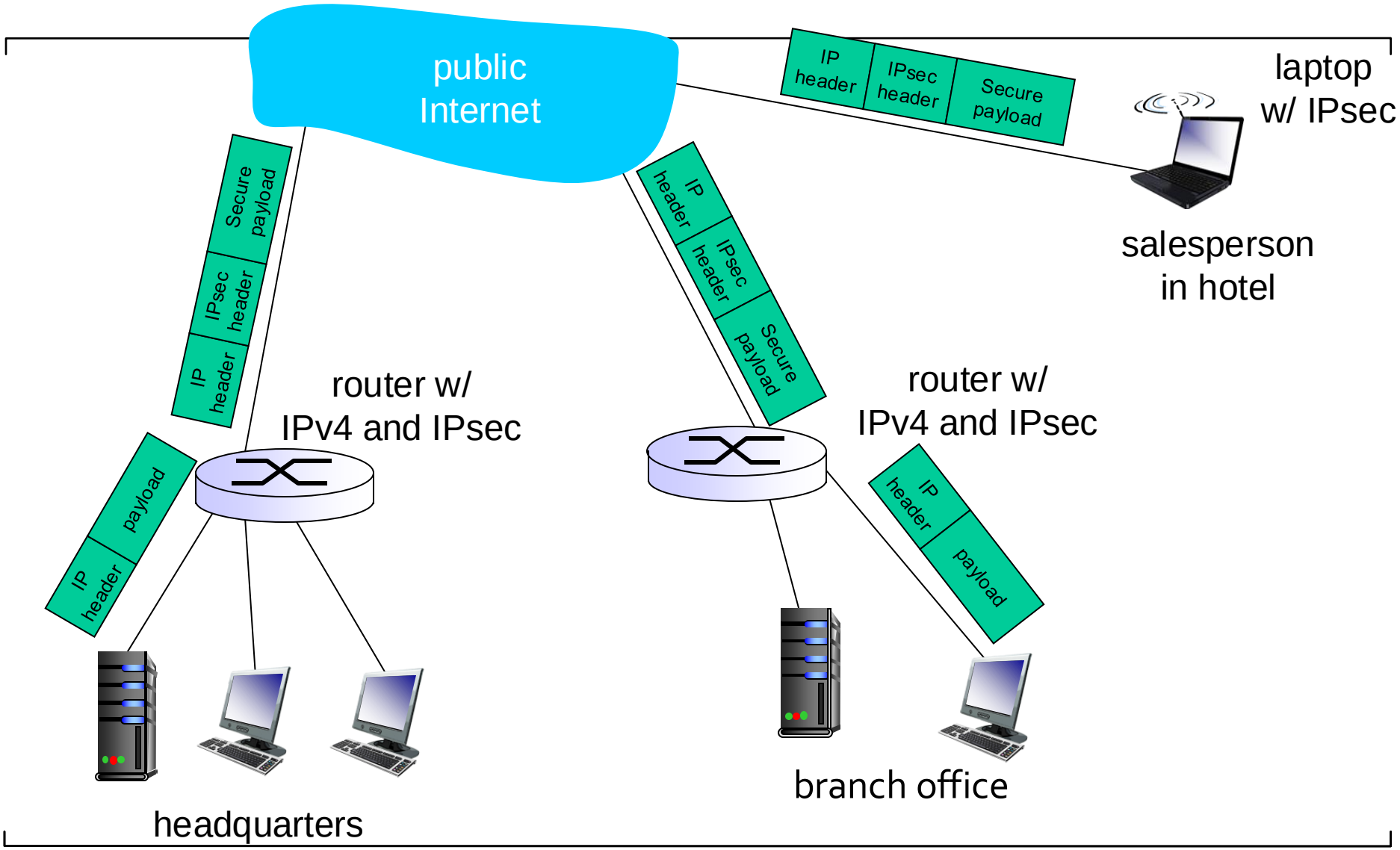
- web pages, e-mail, P2P file transfers, TCP SYN packets …

"blanket coverage"

VPN: institution's inter-office traffic is securely sent over public Internet , where the data is

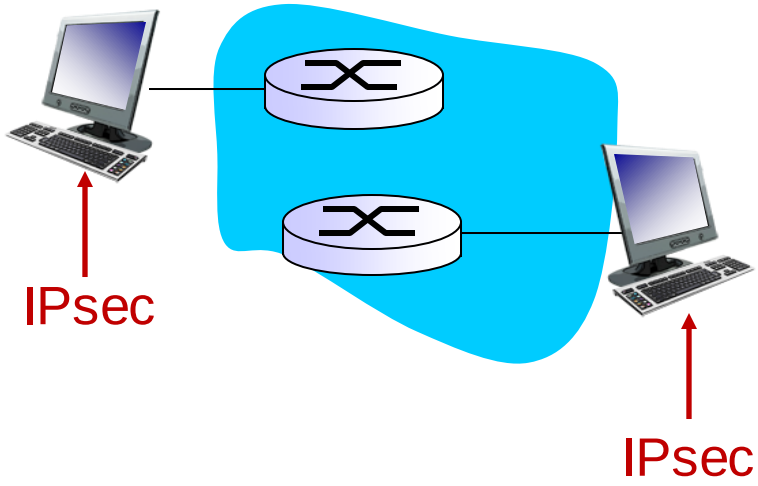
- encrypted before entering the public Internet
- logically separate from other traffic

Virtual Private Networks (VPNs)

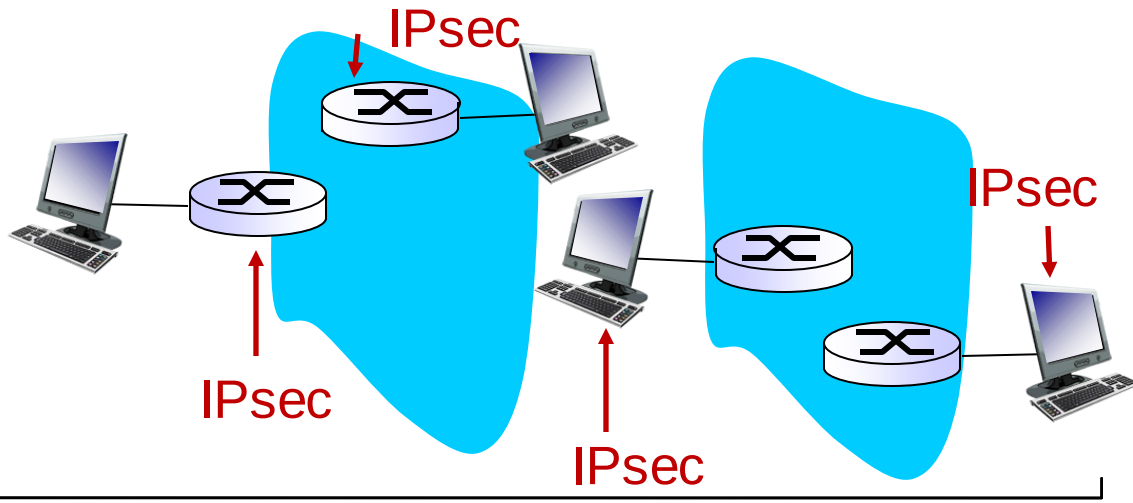


IPsec services

- data integrity, source authentication, confidentiality, and replay attack prevention,. Two modes and Two protocols of IPSec:
- IPsec transport mode:
  - IPsec datagram (encrypted) (not IP header) emitted and received by end-system
  - protects upper-level protocols



- IPsec tunneling mode:
  - Edge router and hosts are IPsec-aware
  - Entire datagram is encrypted and encapsulated



Two IPsec protocols

Authentication Header (AH) protocol

- provides source authentication & data integrity but *not* confidentiality

Encapsulation Security Protocol (ESP)

- provides source authentication, data integrity, *and confidentiality*
- more widely used than AH

Host/ Transport mode with AH	Host/ Transport mode with ESP
Tunnel mode with AH	Tunnel mode with ESP

most common and most important

Security associations (SAs)

before sending data, a network-layer logical connection "security association (SA)" is established from sending to receiving entity

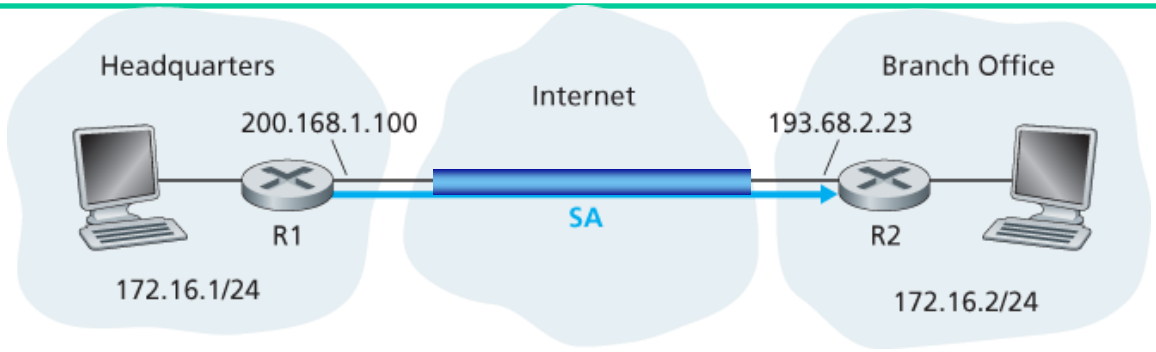
- SAs are simplex: for only one direction, and so two SA's need to be established

ending, receiving entities maintain *state information* about SA

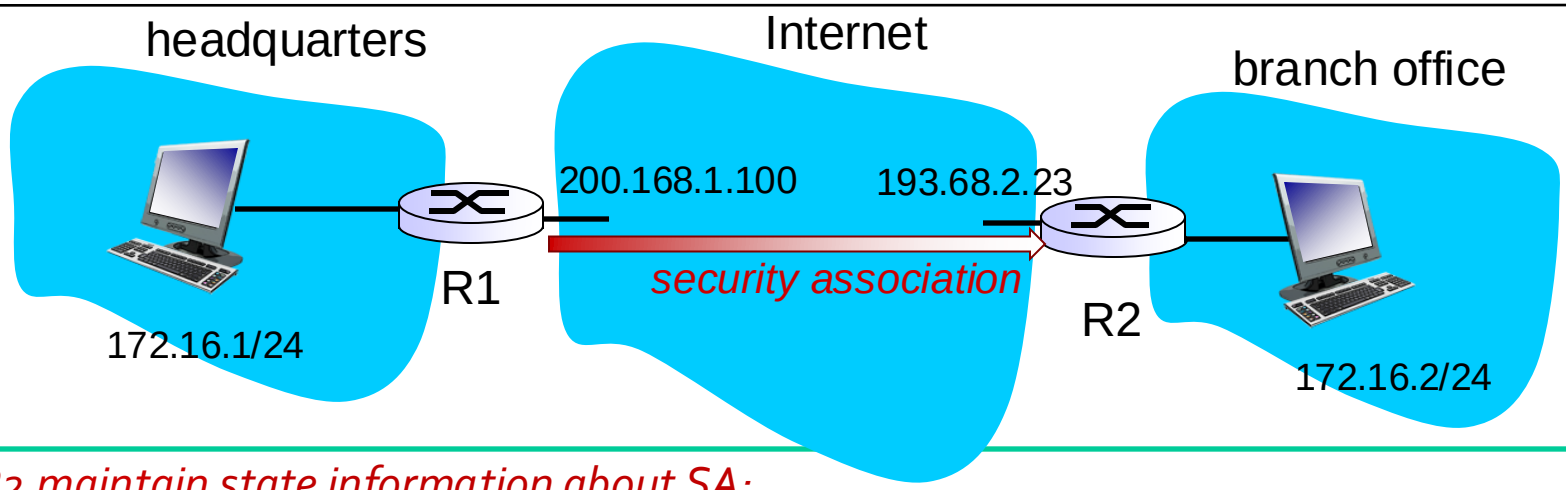
- IP is connectionless but IPsec is connection-oriented!

how many SAs in VPN w/ headquarters (HQ), branch office (BO), and n traveling salespeople (SP)?

2SAs between HQ and BO, 2SAs for each Laptop of traveling SP → (2 + 2n)SAs



Inside SA (from R1 to R2)



R1/ R2 maintain state information about SA:

- 32-bit SA identifier: *Security Parameter Index (SPI)*
- origin SA interface (200.168.1.100)
- destination SA interface (193.68.2.23)
- type of encryption used (e.g., 3DES)
- encryption key
- type of integrity check used (e.g., HMAC with MD5)
- authentication key

Whenever router R1 needs to construct an IPsec datagram for forwarding over this SA, it accesses this state information to determine how it should authenticate and encrypt the datagram. Similarly, router R2 will maintain the same state information for this SA and will use this information to authenticate and decrypt any IPsec datagram that arrives from the SA.

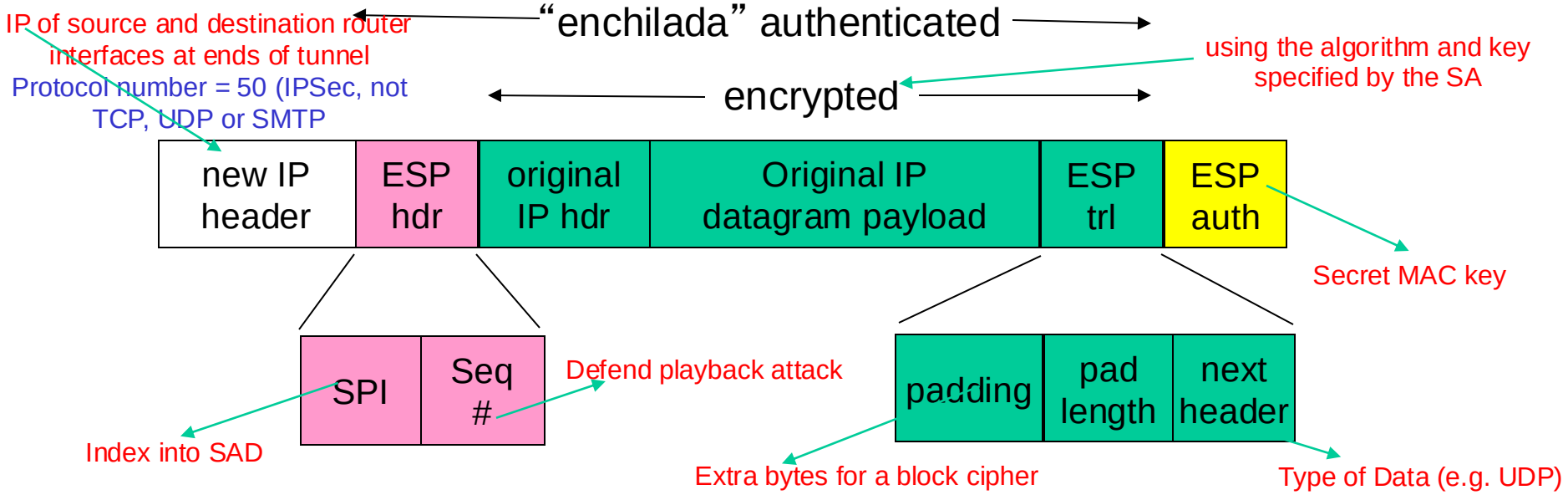
Security Association Database (SAD)

- endpoint holds SA state information in *security association database (SAD)*, where it can locate them during processing.
- data structure in OS kernel of the entity
- when sending IPsec datagram, R1 accesses SAD to determine how to process datagram.
- when IPsec datagram arrives to R2, R2 examines SPI in IPsec datagram, indexes SAD with SPI, and processes datagram accordingly.

with n salespersons, 2 + 2n SAs example:
headquarters gateway router R1 maintains state information for (2+2n) SAs. An IPsec entity stores the state information for all of its SAs in its **SAD**, which is a data structure in the entity's OS kernel.

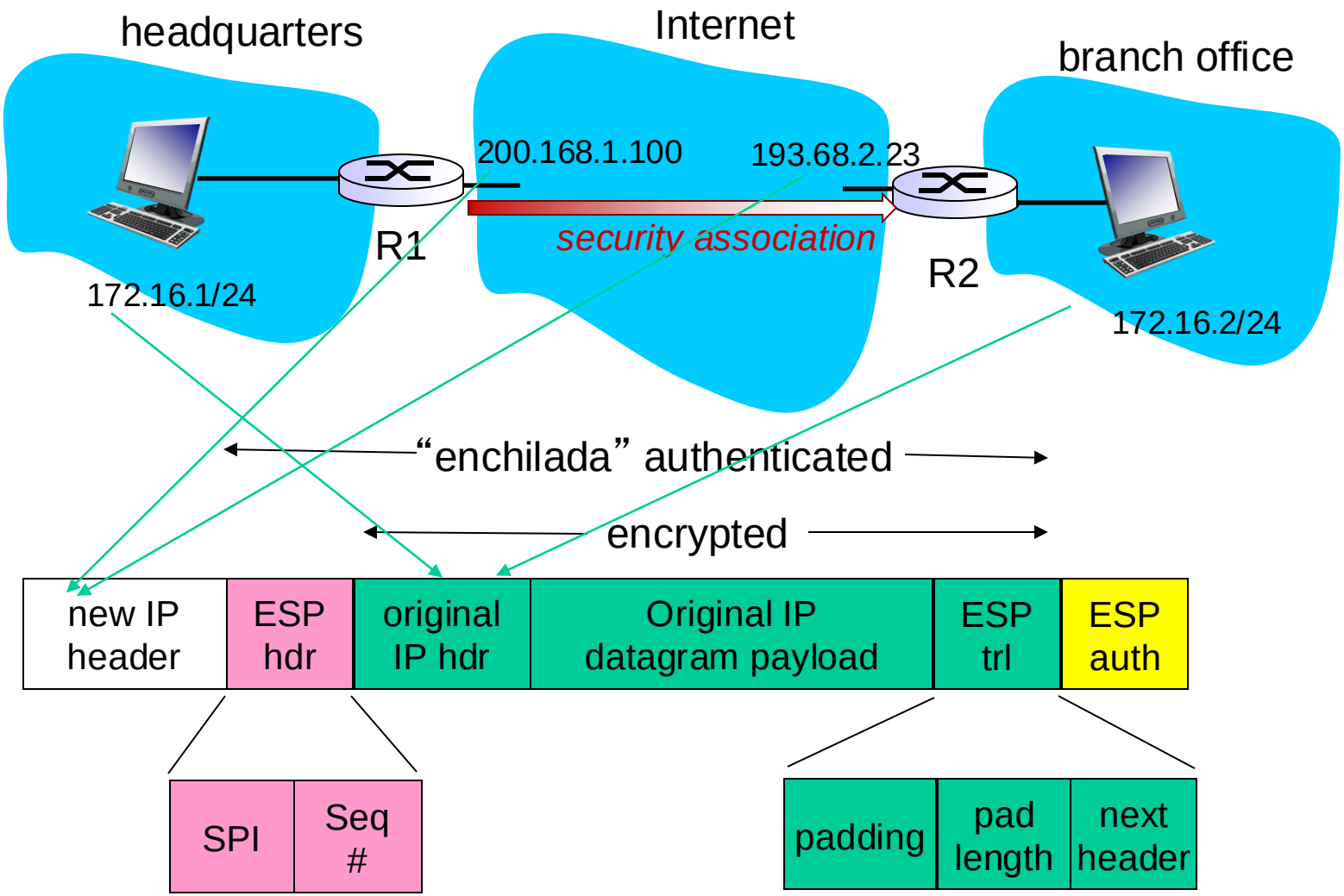
IPsec datagram

IPsec has two different packet forms, one for the **tunnel mode** and the other for the **transport mode.** The tunnel mode with ESP (Encapsulation Security Protocol), being more appropriate for VPNs (Slide 6)



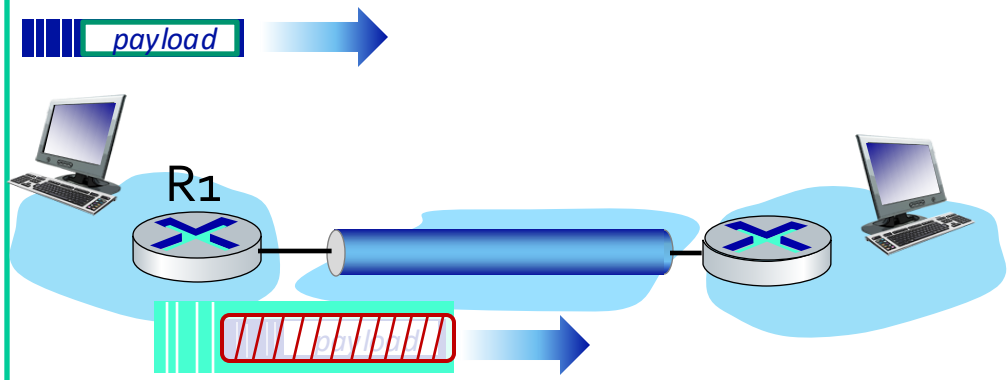
IPsec datagram → "IPv4 datagram" with encrypted payload

Example

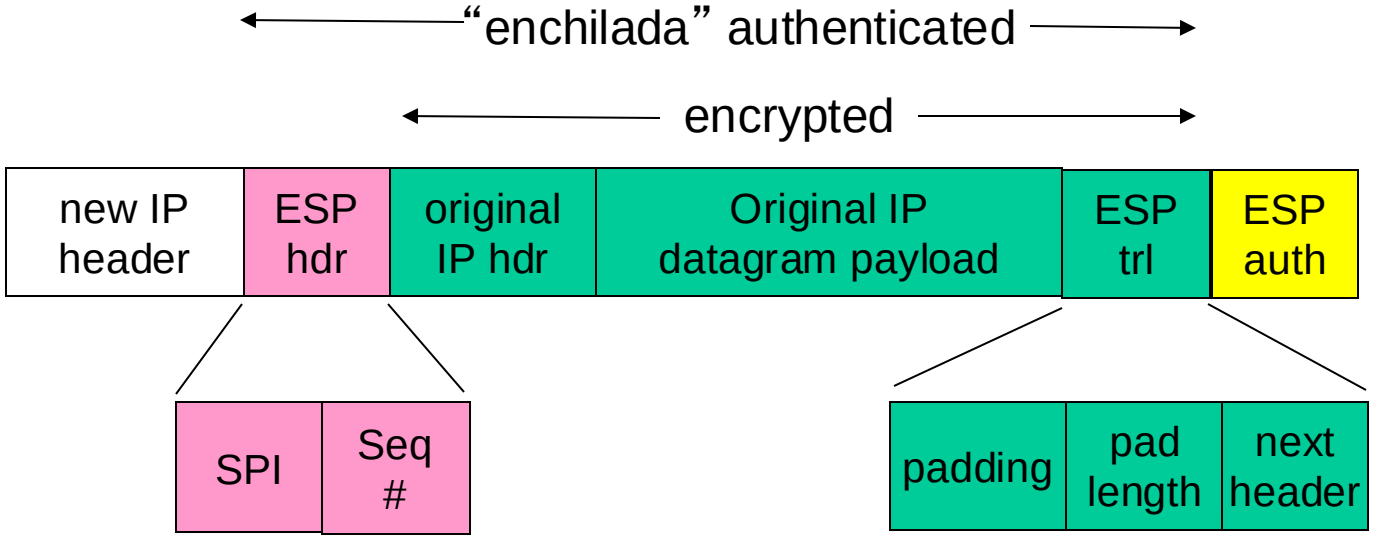

headquarters
Internet
branch office
200.168.1.100
193.68.2.23
R1
security association
R2
172.16.1/24
172.16.2/24
"enchilada" authenticated
encrypted
new IP header
ESP hdr
original IP hdr
Original IP datagram payload
ESP trl
ESP auth
SPI
Seq #
padding
pad length
next header

R1: converts original datagram to IPsec datagram

- appends to back of original datagram (which includes original header fields!) an "ESP trailer" field.
- encrypts result using algorithm & key specified by SA.
- appends to front of this encrypted quantity the "ESP header, creating "enchilada".
- creates authentication MAC over the *whole enchilada*, using algorithm and key specified in SA;
- appends MAC to back of enchilada, forming *payload*;
- creates brand new IP header, with all the classic IPv4 header fields, which it appends before payload



Details:



ESP trailer: Padding for block ciphers

ESP header:

- SPI, so receiving entity knows what to do
- Sequence number, to defend replay attacks

MAC in ESP auth field is created with shared secret key

New IPv4 header field is not set to that of TCP, UDP, or SMTP, but instead to 50, designating that this is an IPsec datagram using the ESP protocol.

The SPI indicates to the receiving entity the SA to which the datagram belongs; the receiving entity can then index its SAD with the SPI to determine the appropriate authentication/decryption algorithms and keys.

IPsec sequence numbers

for new SA, sender initializes seq. # to o

each time datagram is sent on SA:

- sender increments seq # counter
- places value in seq # field

goal:

- prevent attacker from sniffing and replaying a packet
- receipt of duplicate, authenticated IP packets may disrupt service

method:

- destination checks for duplicates
- doesn't keep track of *all* received packets; instead uses a window

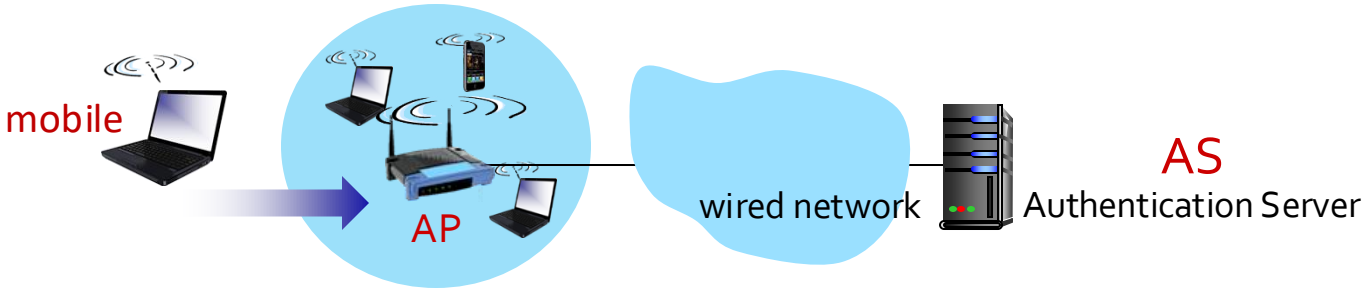
After R1 sends the IPsec datagram into the public Internet, it will pass through many routers before reaching R2. Each of these routers will process the datagram as if it were an ordinary datagram—they are completely oblivious to the fact that the datagram is carrying IPsec-encrypted data. For these public Internet routers, because the destination IP address in the outer header is R2, the ultimate destination of the datagram is R2

R2 processes IPsec datagram

Protocol field (in the left-most IP header) is 50, R2 sees that it should apply IPsec ESP processing to the datagram.

- First, peering into the enchilada, R2 uses the SPI to determine to which SA the datagram belongs.
- Second, it calculates the MAC of the enchilada and verifies that the MAC is consistent with the value in the ESP MAC field. If it is, it knows that the enchilada comes from R1 and has not been tampered with.
- Third, it checks the sequence-number field to verify that the datagram is fresh (and not a replayed datagram).
- Fourth, it decrypts the encrypted unit using the decryption algorithm and key associated with the SA.
- Fifth, it removes padding and extracts the original IP datagram
- Sixth, it forwards the original datagram into the branch office network toward its ultimate destination.

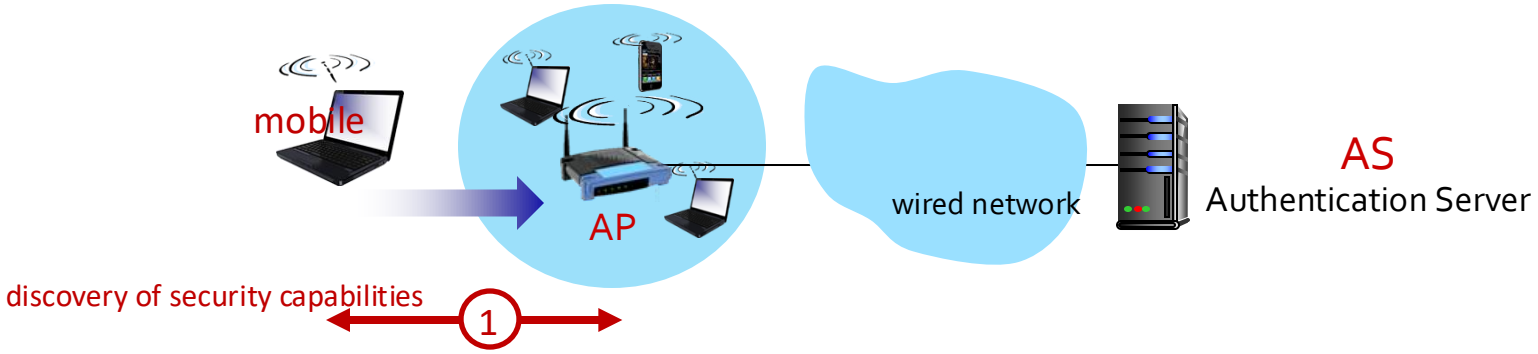
Security in Wireless Networks 802.11: authentication, encryption



Arriving mobile must:

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

802.11: authentication, encryption

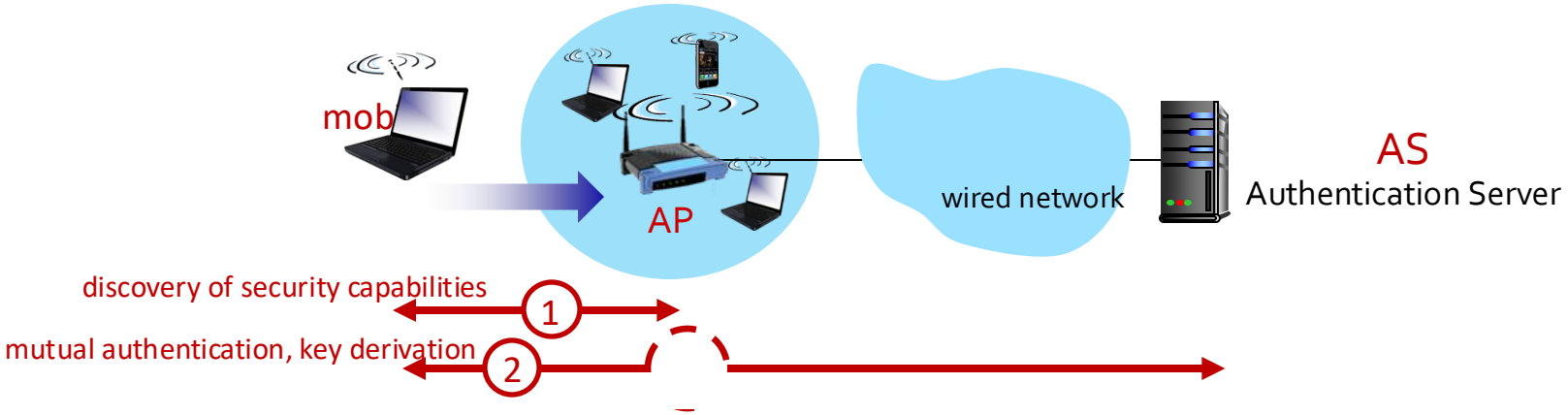


1 discovery of security capabilities:

- AP advertises its presence, forms of authentication and encryption provided
- device requests specific forms authentication, encryption desired

although device, AP already exchanging messages, device not yet authenticated, does not have encryption keys

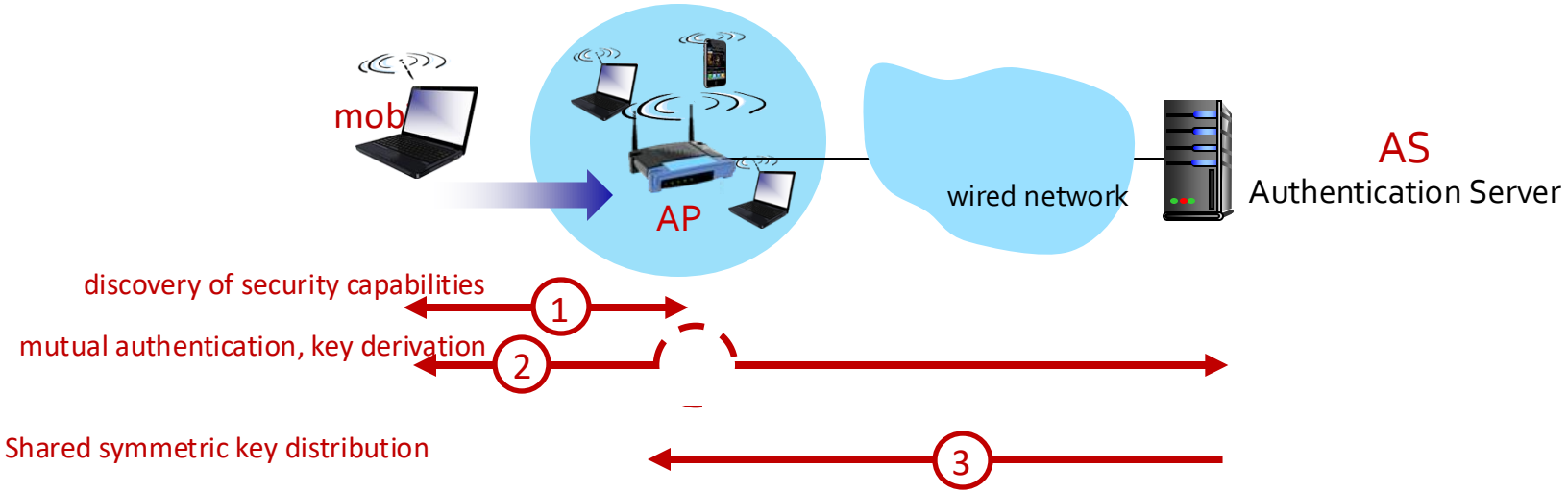
802.11: authentication, encryption



(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 authenticating each other
- AS, mobile derive symmetric session key

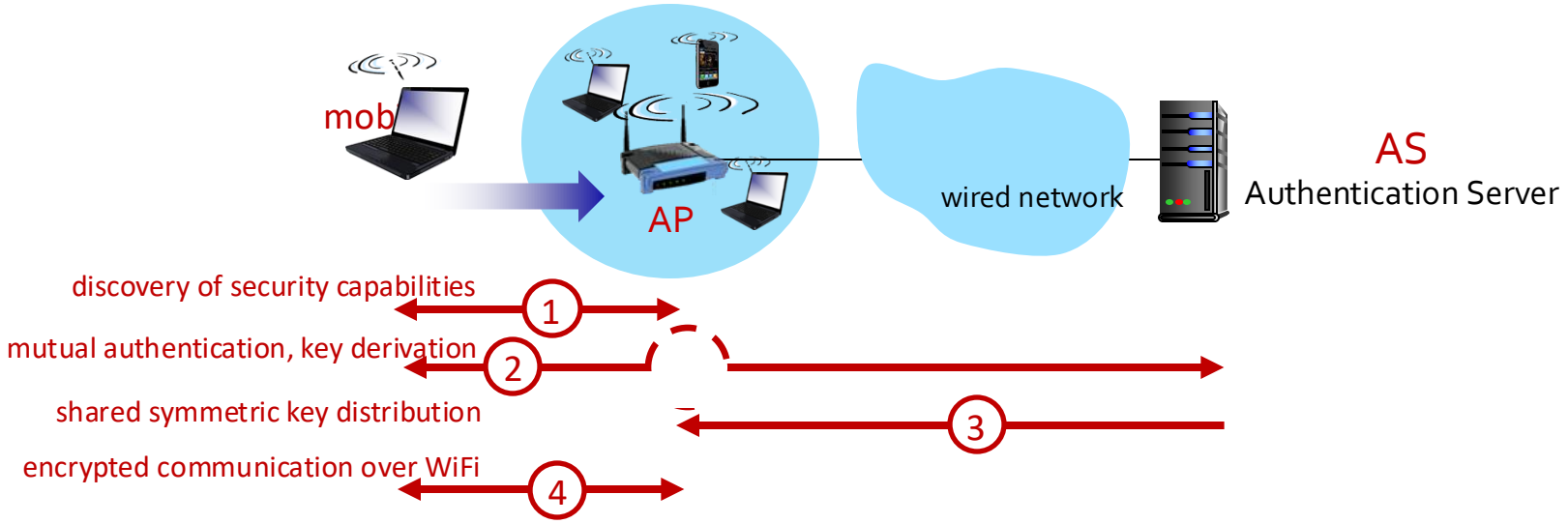
802.11: authentication, encryption



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

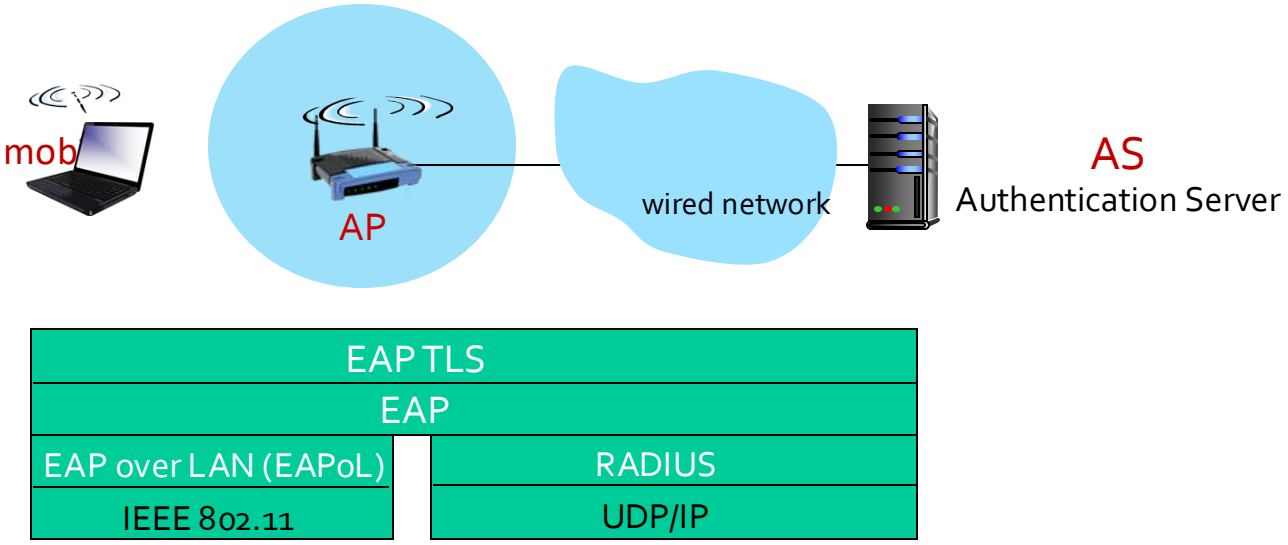
802.11: authentication, encryption



4 encrypted communication between mobile and remote host via AP

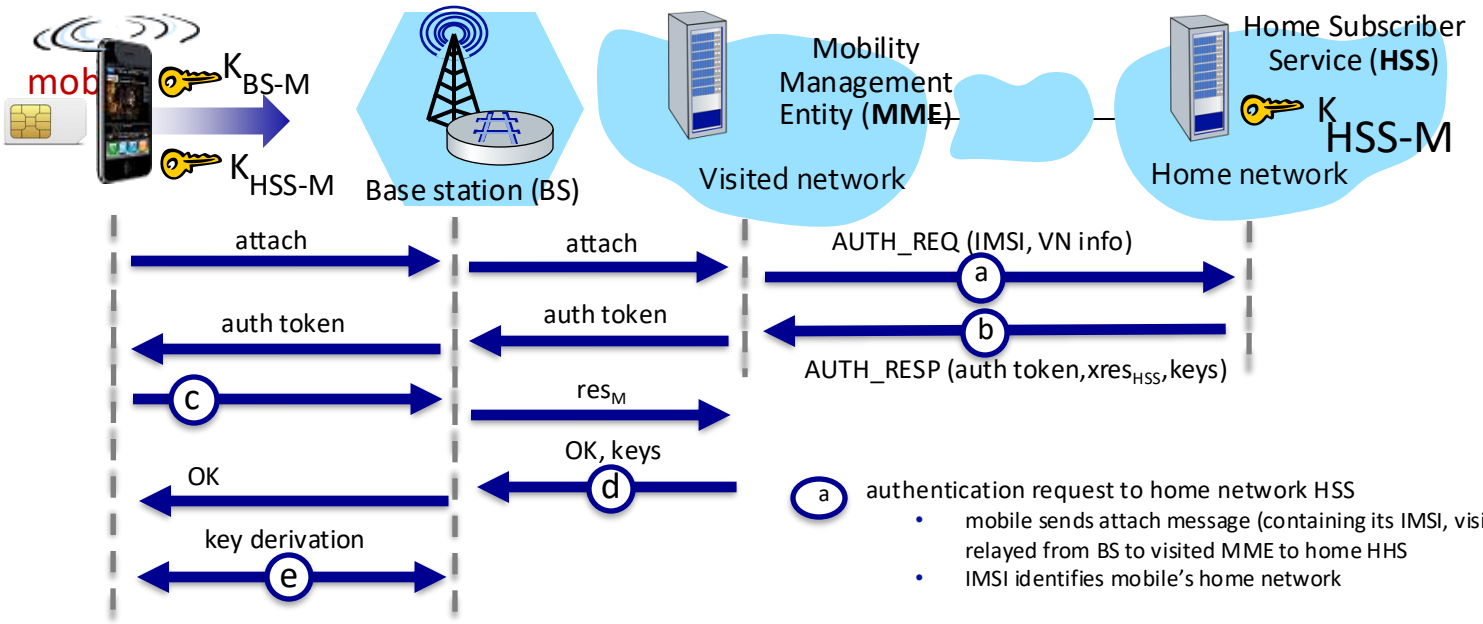
- same key derived at mobile, AS
- AS informs AP of the shared symmetric session

802.11: authentication, encryption



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

Authentication, encryption in 4G LTE



a authentication request to home network HSS
- mobile sends attach message (containing its IMSI, visited network info) relayed from BS to visited MME to home HHS
- IMSI identifies mobile's home network

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

c
- authentication response from mobile:
  - mobile computes res_M using its secret key to make same cryptographic calculation that HSS made to compute $xres_{HSS}$ and sends res_M to MME

d
- mobile is authenticated by network:

e mobile, BS determine keys for encrypting data, control frames over 4G wireless channel → AES can be used

Authentication, encryption: 4G to 5G

4G: MME in visited network makes authentication decision

5G: home network provides authentication decision

- visited MME plays "middleman" role but can still reject

4G: uses shared-in-advance keys

5G: keys not shared in advance for IoT

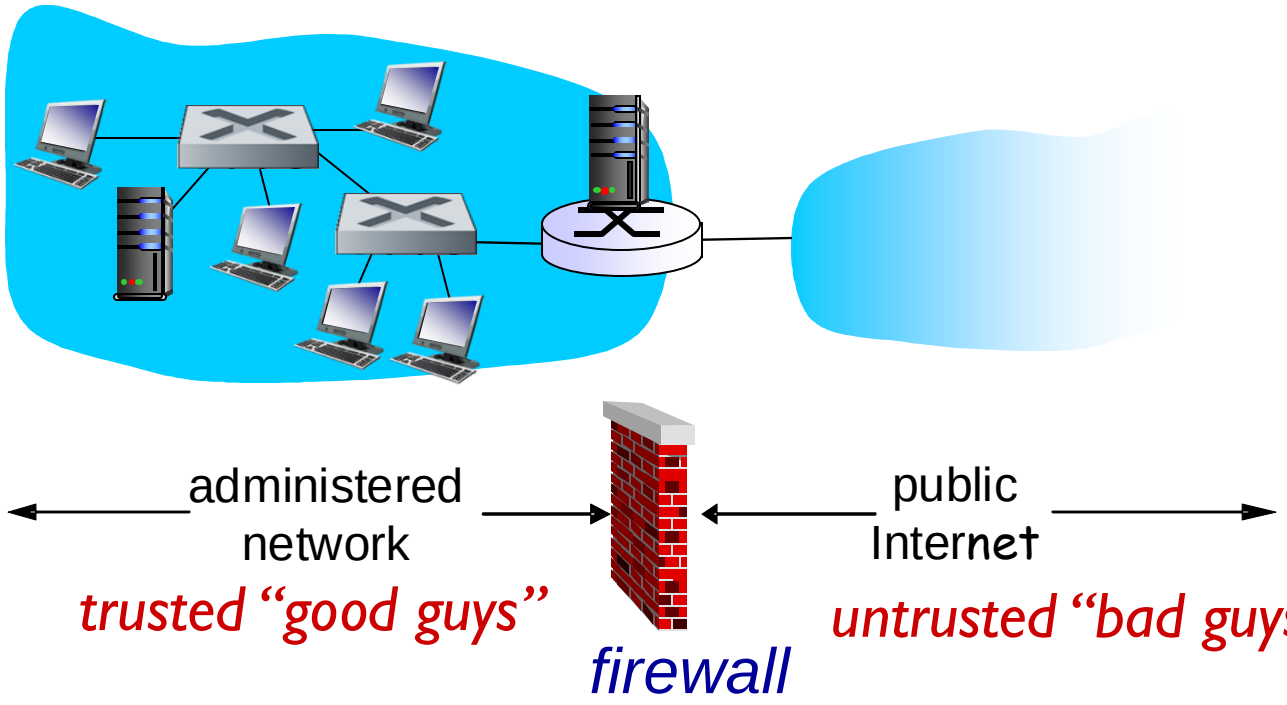
4G: device IMSI transmitted in cleartext to BS

5G: public key crypto used to encrypt IMSI

Operational Security
Firewalls

firewall

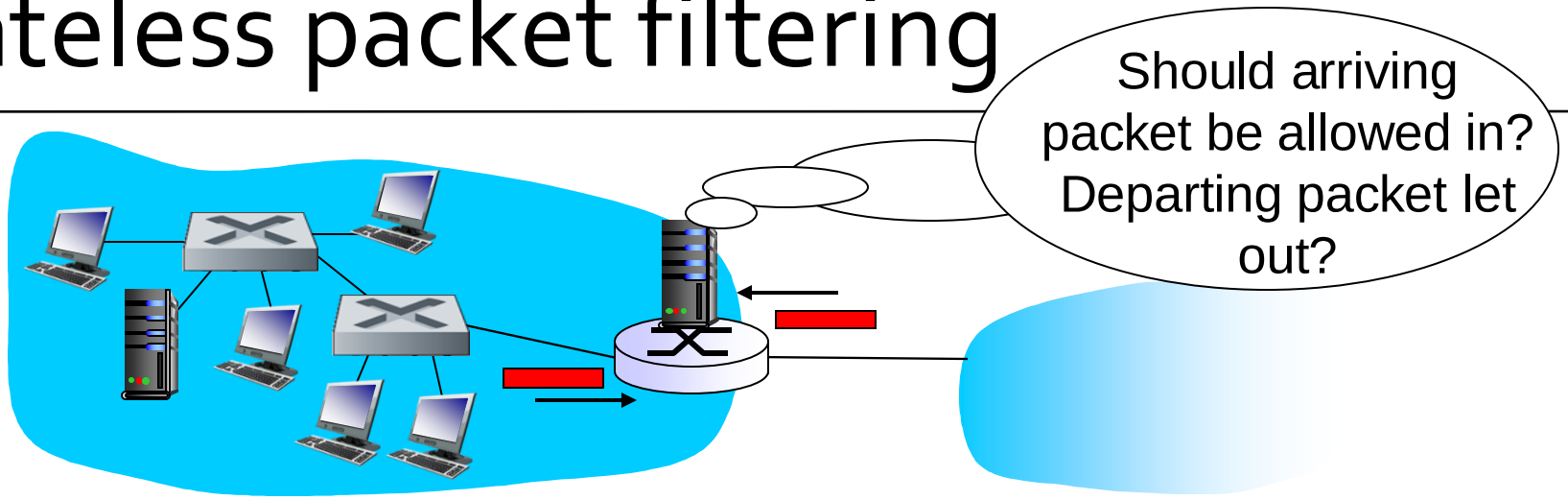
isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



Firewalls: why

- prevent denial of service attacks:
  - SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections
- prevent illegal modification/access of internal data
  - e.g., attacker replaces institution's homepage with something else
- allow only authorized access to inside network
  - set of authenticated users/hosts
- three types of firewalls:
  - traditional (stateless) packet filters
  - stateful packet filters
  - application gateways

Stateless packet filtering



internal network connected to Internet via *router firewall*

router *filters packet-by-packet,* decision to forward/drop packet based on:

- source IP address, destination IP address
- TCP/UDP source and destination port numbers
- ICMP message type
- TCP SYN and ACK bits

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

ACL: table of rules, applied top to bottom to incoming packets: (action, condition) pairs: looks like OpenFlow forwarding

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Stateful packet filtering

In a traditional packet filter, filtering decisions are made on each packet in isolation. Stateful filters actually track TCP connections, and use this knowledge to make - filtering decisions.

stateless packet filter: heavy handed tool

- admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

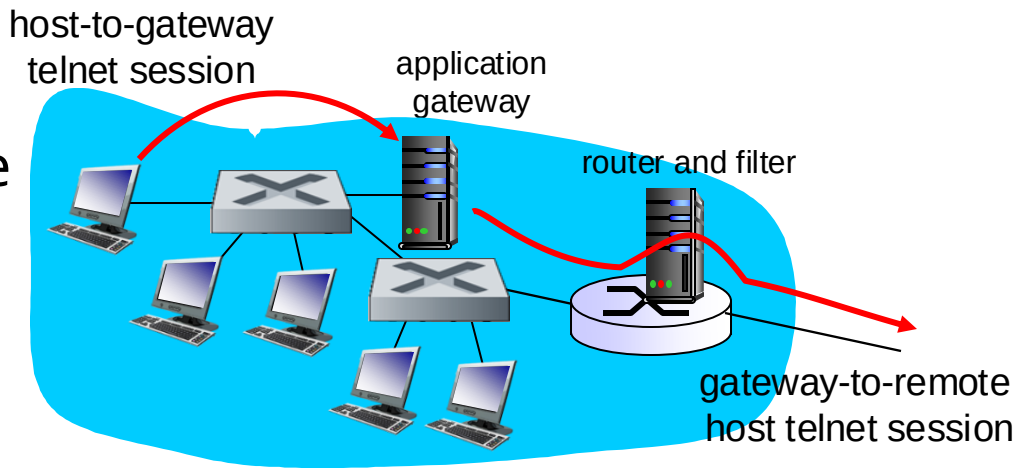
action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

stateful packet filter: track status of every TCP connection

- track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
- timeout inactive connections at firewall: no longer admit packets

Application gateways

Filter packets on application data as well as on IP/TCP/UDP fields, to ensure conformity to application specifications



Example: allow select internal users to telnet outside

1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Intrusion detection systems

packet filtering:

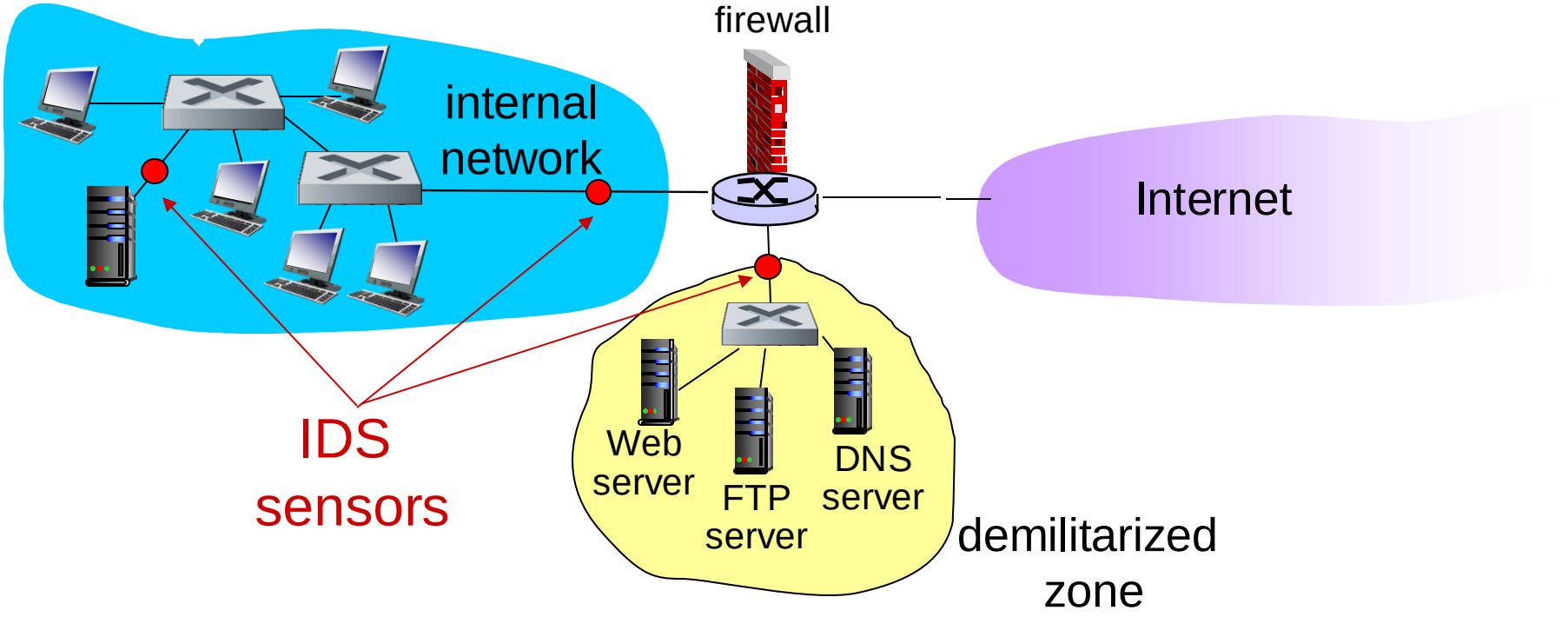
- operates on TCP/IP headers only
- no correlation check among sessions

IDS: intrusion detection system

- *deep packet inspection:* look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
- examine correlation among multiple packets
  - port scanning
  - network mapping
  - DoS attack

Intrusion detection systems

multiple IDSs: different types of checking at different locations



Network Security (summary)

basic techniques……

- cryptography (symmetric and public)
- message integrity
- end-point authentication

…. used in many different security scenarios

- secure email
- secure transport (TLS)
- IP sec
- 802.11

operational security: firewalls and IDS

Summary

Today:

- VPN
- IPsec datagram and services
- Wireless
- Firewalls, gateways, and IDS

Canvas discussion:

- Reflection
- Exit ticket

Next:

- Final Exam
- follow on Canvas! material and announcements
- Contribute to SCU course evaluation

Any questions?