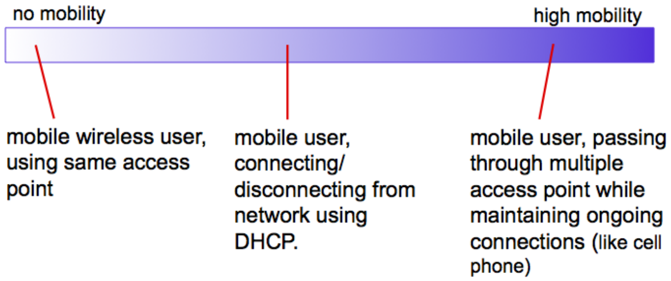
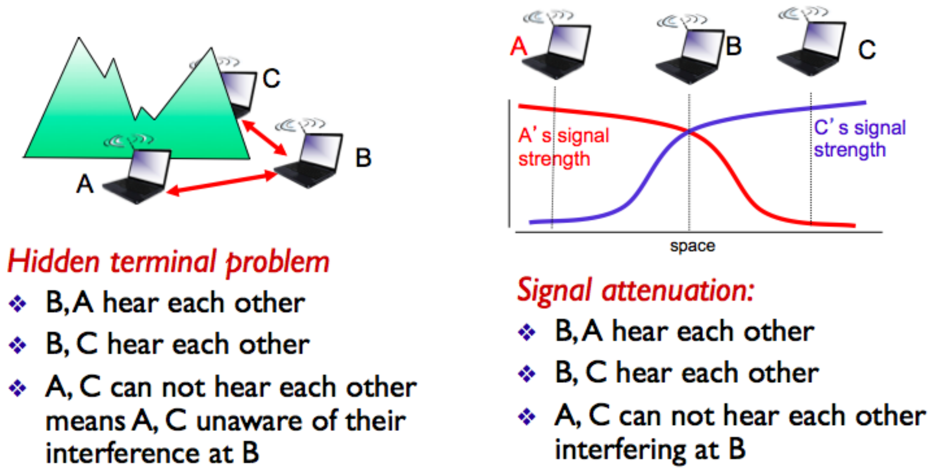
LOOK AT ALL THESE BUSY BEE'S!! GOOD LUCK EVERYONE...

Overview (Kurose Chs. 6, 8) You should be able to:

- (Ch 6) Wireless Communication & Mobility
  - Wireless
    - communication over wireless link.
  - Mobility
    - Handling the mobile user who changes point of attachment to the network.
    - Spectrum of mobility, from the network perspective.
    - 
no mobility
high mobility
mobile wireless user, using same access point
mobile user, connecting/ disconnecting from network using DHCP.
mobile user, passing through multiple access point while maintaining ongoing connections (like cell phone)
  - Hosts
    - laptop, smartphone
    - run applications
    - stationary (non-mobile) or mobile
  - Links
    - Used to connect mobiles to base station
    - multiple access protocol coordinates link access
    - various data rates, transmission distance
  - Base stations
    - Typically connected to wired network
    - relay - send packets between wired network and wireless hosts in its "area" - e.g. cell towers, 802.11 access points, routers
  - Network infrastructure
    - base station connects mobiles into wired network
    - handoff: mobile changes base station providing connection into wired network
  - Wireless Link/Network characteristics:
    - Decreasing signal strength
      - Radio signal attenuates as it propagates through matter (path loss)
      - Inverse Squared vs Wired - Doubling the distance from the emitter attenuates the signal by 1/4th
    - Interference from other sources
      - Standardized wireless network frequencies (2.4 GHz) shared by other devices (phone); devices (motors) interfere as well
    - Multipath propagation
      - Radio signal reflects off objects ground, arriving at destination at slightly diff times
  - What makes communication across a wireless network more "difficult?" ANS. Below
  - Signal to noise ratio (SNR)
    - larger = good: easier to extract signal from noise.
    - As SNR increases, bit-error rate decreases.

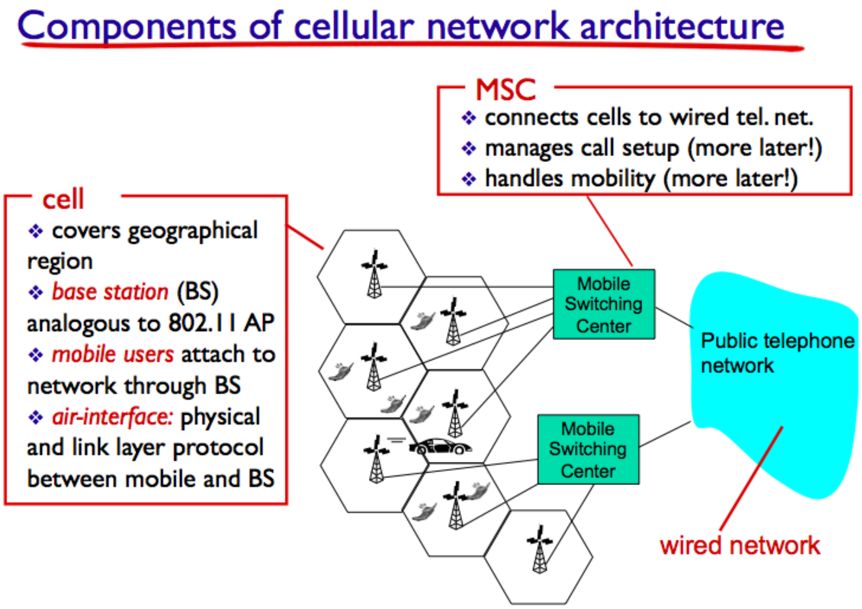
- 

  Hidden terminal problem
  - B,A hear each other
  - B, C hear each other
  - A, C can not hear each other means A, C unaware of their interference at B

  Signal attenuation:
  - B,A hear each other
  - B, C hear each other
  - A, C can not hear each other interfering at B
- Code Division Multiple Access (CDMA)
  - unique “code” assigned to each user; i.e code set partitioning
    - users share frequency but each user has own “chipping” sequence (i.e. code) to encode data
    - allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
  - encoded signal: (original data) x (chipping sequence)
  - decoding: inner-product of encoded signal and chipping sequence

- 802.11 Wireless LAN
  - wireless host communicates with base station
    - base station = access point (AP)
  - Basic Service Set (BSS) (aka “cell”) in infrastructure mode contains:
    - wireless hosts
    - access points aka “base stations”
    - ad hoc mode: hosts only
  - Active Scanning: proves requests/creates traffic, via switch.
    - Switches avoid collisions
  - Passive Scanning: waits for traffic from hosts, via a hub.
    - Hubs allow collisions
- 802.11 MAC protocols
  - Carrier Sense Multiple Access (CSMA)
    - sense before transmission
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
    - nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle".[1][2] When they do transmit, nodes transmit their packet data in its entirety.
    - Sender Steps
      - If sense channel idle for distributed inter-frame space (DIFS) then transmit packet.
      - If sense channel busy then start random backoff time. When timer ends, check for ACK from receiver then repeat timer if no ACK.
    - Receiver Steps
      - if frame received OK then reply with ACK after short interframe space (SIFS).

    - Request to Send (RTS) used to AVOID COLLISIONS
        - allows sender to “reserve” channel rather than random access of data frames.
        - sender first transmits small request to send (RTS) packets to BS using CSMA
        - BS broadcasts clear-to-send (CTS) in response to RTS.
    - Clear-to-send (CTS)
        - heard by all nodes
        - sender transmits data frame
        - other stations defer transmissions
    - AVOID COLLISIONS COMPLETELY USING SMALL RESERVATION PACKETS.
    - Beacon Frame: management frame containing all information about network.
- Bluetooth (IEEE 802.15 - Personal Area Network)
    - no infrastructure = ad hoc, peer to peer
    - “master/slave” relationships

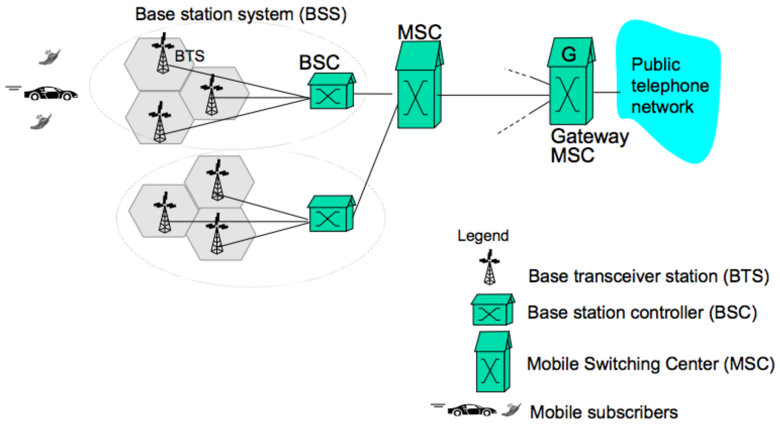


Components of cellular network architecture

MSC
- connects cells to wired tel. net.
- manages call setup (more later!)
- handles mobility (more later!)

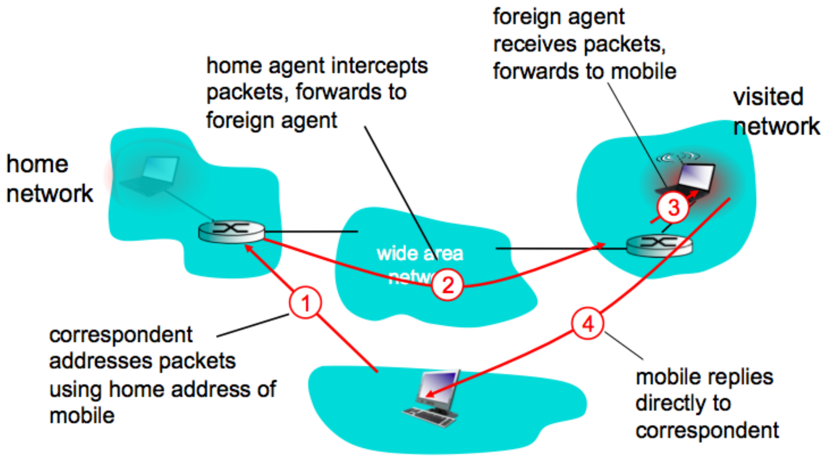
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS

- Wimax (World Interoperability for Microwave Access)
    - A family of IEEE 802.16 standards that is competing with 4G-LTE but differ significantly.
- Cellular access
    - 2G (Voice)

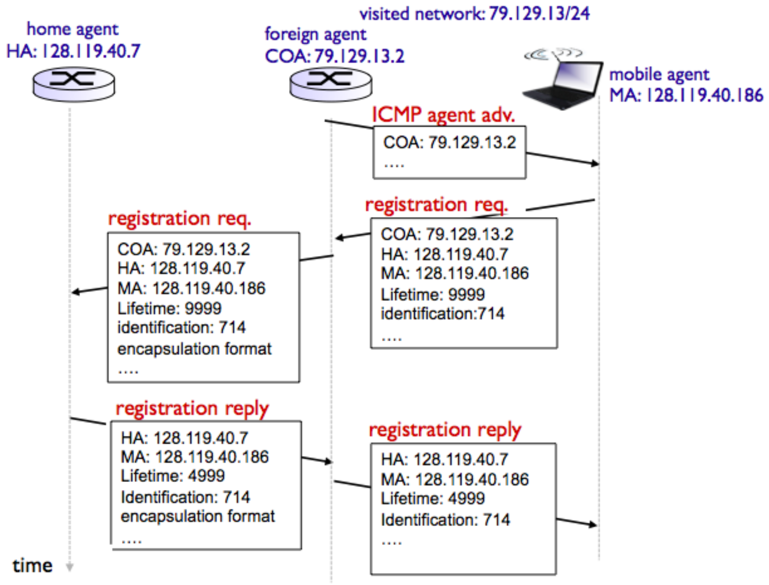

Base station system (BSS)
BTS
BSC
MSC
G
Public telephone network
Gateway MSC
Legend
Base transceiver station (BTS)
Base station controller (BSC)
Mobile Switching Center (MSC)
Mobile subscribers

    - 2.5G
        - 2G networks that have incorporated a packet-switched domain in addition to the circuit-switched domain.
    - 3G (Voice+Data)

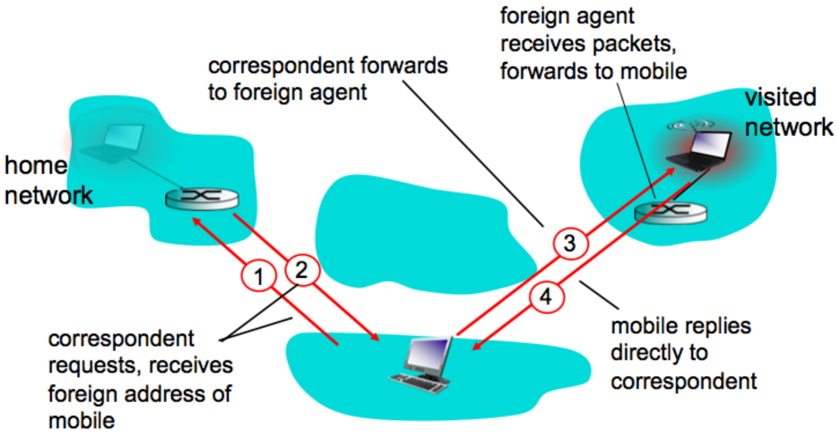
      - new cellular data network operates in parallel with original voice (2G) network.
    - 4G-LTE (long-term evolution) - two important innovations:
      - Evolved Packet Core (EPC) - simplified all-IP core network that unifies the circuit-switched voice net and the packet-switched cellular data net
      - LTE Radio Access Network - combo of frequency division multiplexing and time division - OFDM (orthogonal frequency division multiplexing) - very little interference
        - sophisticated MIMO (multi input, multi output) antennas
  - Mobility
    - Home agent
      - entity that will perform mobility functions on behalf of mobile, when mobile is remote
    - Foreign agent
      - entity in visited network that performs mobility functions on behalf of mobile
    - COA (care-of-address)
      - Address in visited network
      - Used by home agent to forward datagrams to mobile
  - Mobile IP
    - Internet architecture and protocols for supporting mobility
    - Three components to standard
      - Indirect routing of datagrams
        - communication from correspondent to mobile goes through home agent, then forwarded to foreign agent, then to mobile. Known as “triangle routing”


foreign agent receives packets, forwards to mobile
home agent intercepts packets, forwards to foreign agent
visited network
home network
wide area netw
1
2
3
4
correspondent addresses packets using home address of mobile
mobile replies directly to correspondent

      - Agent Discovery
        - “agent advertisement” sent by foreign/home agents broadcast ICMP message, typefield 9.
      - Registration w/ Home Agent



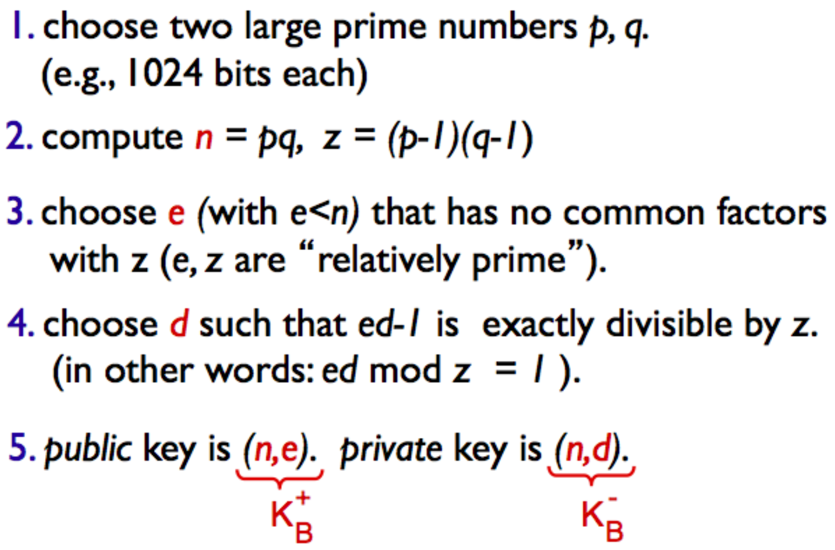
- Mobile Routing
    - indirect routing: communication from correspondent to mobile goes through home agent, then forwarded to remote. Known as “triangle routing”
        - Permanent Address: used by correspondent, hence mobile location transparent to correspondent)
        - Care-of-Address: used by home agent to forward datagrams to mobile.
    - direct routing: correspondent gets foreign address of mobile, communicates directly to mobile.



- Handoffs
    - Goal: route call via new base station, without interruption.
    - Reasons for handoff
        - strong signal to/from new BSS.
        - load balance: free up channel in current BSS
        - GSM doesn’t mandate why to perform handoff (policy), only how (mechanism).
        - Handoff initiated by old BSS.

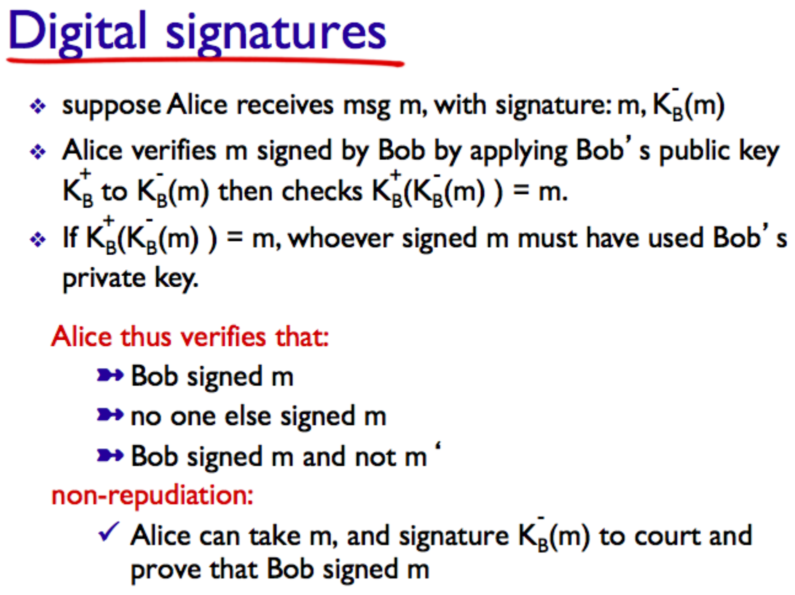
- (Ch 8) Network Security
    - Confidentiality
        - Only sender, intended receiver should “understand” message contents
            - sender encrypts message
            - receiver decrypts message
    - Authentication

        - sender, receiver want to confirm identity of each other. Verifies, “you are who you claim to be.”
    - Message integrity
        - sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
    - Authorization/Access and availability
        - services must be accessible and available to users.
    - Operational security
        - Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)
- Eavesdropping
    - intercept messages
- Modification
    - changing message contents, man in the middle attack.
- Insertion or deletion of messages
    - Can potentially be performed by an intruder
- Cryptography:
    - Encryption - changing plaintext to ciphertext through use of an encryption algorithm
    - Plaintext - message in its original form
    - Ciphertext - Encrypted message: unintelligible to any intruder
- Symmetric Key Cryptography
    - Sender and receiver share same (symmetric) encryption/decryption keys.
    - Data Encryption Standard (DES)
        - creates 56-bit symmetric key, from 64-bit plaintext input.
        - not very secure, improved by 3DES; 3 encryptions with 3 different keys.
    - Advanced Encryption Standard (AES)
        - replaced DES in Nov. 2001.
        - process data in 128-bit blocks.
        - 128, 192, 256-bit keys
- Caesar cipher
    - Very old and simple symmetric key algorithm, form of substitution encryption cipher.
    - Substitute each letter in the plaintext message with letter that is *k* letters later/previous
- Monoalphabetic cipher
    - Improves on Caesar cipher
    - substitute one letter for another.
- Block cipher
    - message to be encrypted is processed in blocks of *k* bits
    - Each block encrypted independently using 1 : 1 mapping (different output for each input)
        - Possible mappings = permutation of inputs (8 possible inputs, 8! mappings = 40,320)
- Public key encryption
    - Public Key Cryptography
        - sender, receiver do not share secret key
        - public encryption key known to all (Kb+)
        - private decryption key known <u>only</u> to receiver (Kb-)
    - need Kb+ and Kb- such that Kb-(Kb+(m)) = m
    - given public key Kb+ it should be impossible to compute private key Kb-
- Rivest, Shamir, Adelson algorithm (RSA)
    - Integral part of Public Key Cryptography
    - Determining public and private keys

- 

  1. choose two large prime numbers *p, q.* (e.g., 1024 bits each)
  2. compute $n = pq$, $z = (p-1)(q-1)$
  3. choose e (with $e<n$) that has no common factors with z (e, z are "relatively prime").
  4. choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).
  5. *public* key is $\underbrace{(n,e)}_{K_B^+}$. *private* key is $\underbrace{(n,d)}_{K_B^-}$.
- Public key is pair of numbers (n,e); private key is pair of number (n,d)
- To encrypt: c = m^e mod n, where c is ciphertext
- To decrypt: m = c^d mod n, where m is message
- Works because there are no known algorithms for quickly factoring a prime number
- Session Keys
    - Bob & Alice use RSA to exchange a symmetric key Ks.
    - Once both have Ks, they use symmetric key cryptography because its so much faster.

- Message integrity
    - Verify the message was originated from correct sender
    - Verify message was not tampered on its way to receiver
    - Digital Signatures
        - cryptographic technique analogous to hand-written signatures. Cannot be forged.



Digital signatures

- suppose Alice receives msg m, with signature: m, $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- If $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

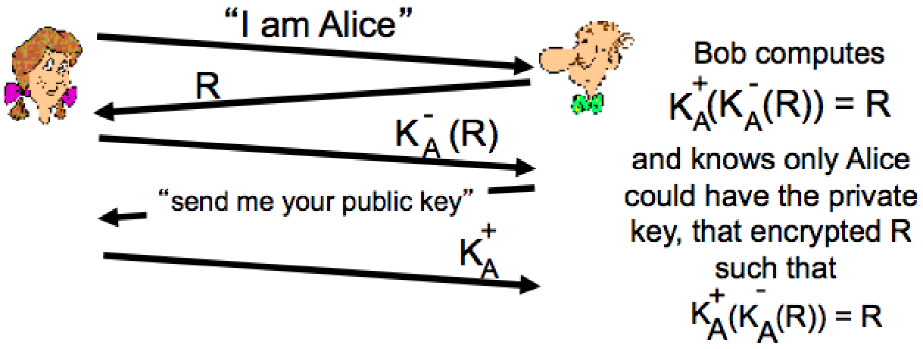
- Bob signed m
- no one else signed m
- Bob signed m and not m'

non-repudiation:

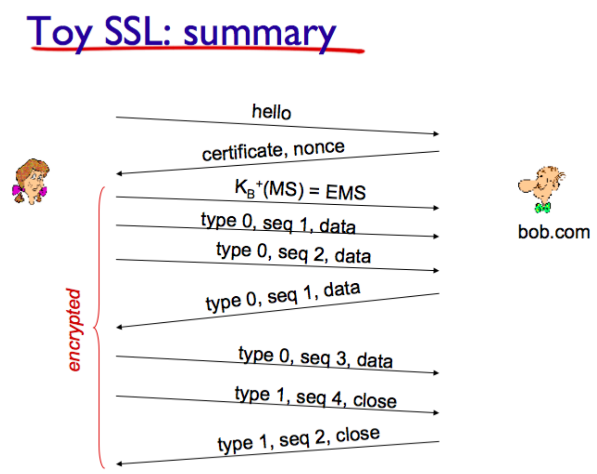
- ✓ Alice can take m, and signature $K_B^-(m)$ to court and prove that Bob signed m

- Authentication
    - Nonce, number used once-in-a-lifetime.
        - Used to avoid playback attack.
        - number(R) used only once in a lifetime
        - avoid playback attack
    - Ap5.0 requires shared symmetric key in addition to nonce.

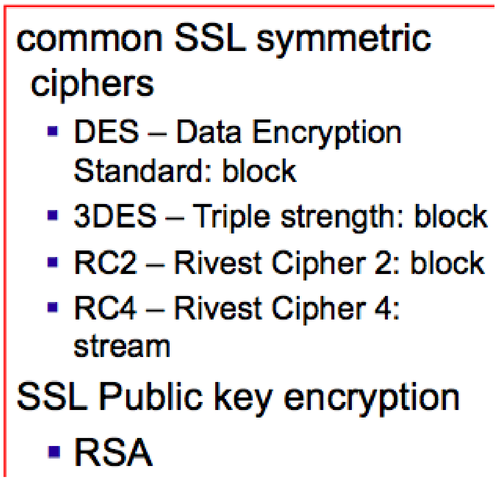
        - security hole: man in the middle attack (MITM)


"I am Alice"
R
$K_A^-(R)$
"send me your public key"
K_A^+
Bob computes
$K_A^+(K_A^-(R)) = R$
and knows only Alice could have the private key, that encrypted R such that
$K_A^+(K_A^-(R)) = R$

- Cryptographic Hash Functions
    - Hash function takes an input *m* and computes a fixed size string H(m) called a hash - Internet checksum and Cyclic Redundancy Check (CRC)
    - Cryptographic hash function has additional property
        - Computationally infeasible to find any 2 different messages x and y s.t. H(x) = H(y)
        - Intruder can't substitute one message for another message that is protected by the hash function
    - MD5 hash function widely used (RFC 1321).
- Public key certification
    - Certify that a public key belongs to a specific entity
    - Certificate Authority (CA)
        - Bind public key to particular entity, E
        - Verifies that an entity is who it says it is
- Endpoint authentication
    - Process of one entity proving its identity to another entity over a computer network
- E-mail:
    - PGP (Pretty Good Privacy) - email encryption scheme that has become de facto standard
        - uses MD5 or SHA for calculating message digest; CAST, triple-DES, or IDEA for symmetric key encryption; and RSA for public key encryption.
    - To ensure secrecy, sender authentication, and message integrity. Sender must use all three keys; sender's private key, receiver's public key, newly created symmetric key.
- Secure Socket Layer (SSL) - Transport layer security
    - widely deployed security protocol - supported by almost all browsers (https)
    - provides: confidentiality, integrity, authentication
    - Original goals
        - web e-commerce transactions
        - encryption
        - web-server authentication
        - optional client authentication
        - minimum hassle in doing business with new merchant
    - Available to all TCP applications



Toy SSL: summary

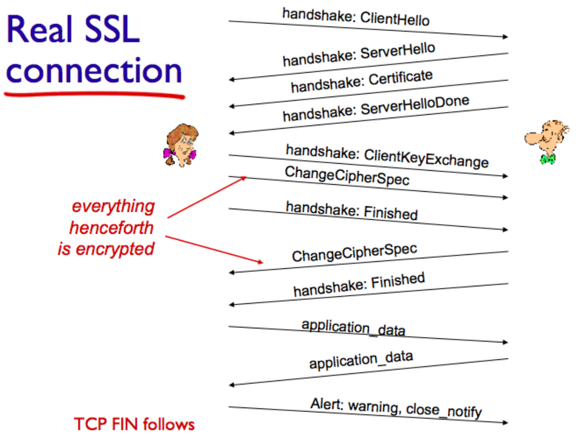


common SSL symmetric ciphers

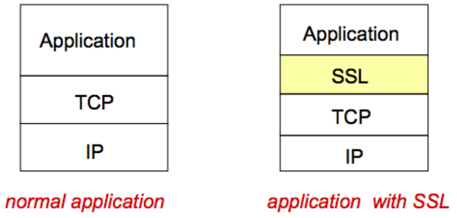
- DES – Data Encryption Standard: block
- 3DES – Triple strength: block
- RC2 – Rivest Cipher 2: block
- RC4 – Rivest Cipher 4: stream

SSL Public key encryption

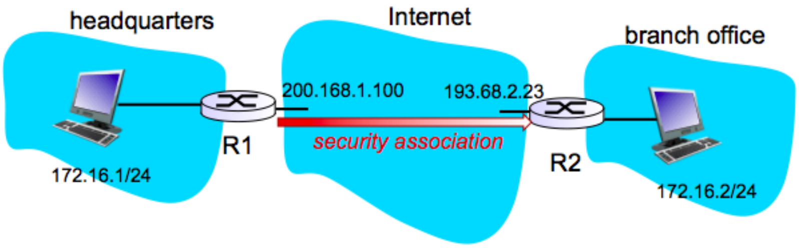
- RSA

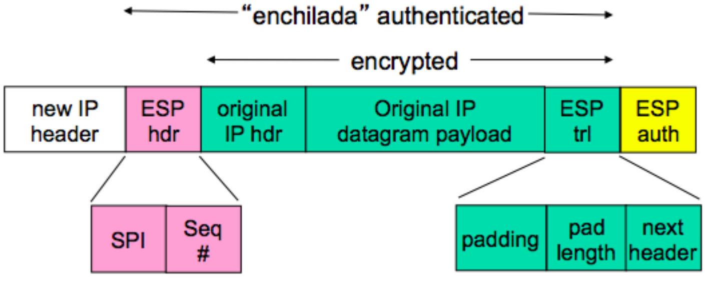


Real SSL connection



- IP Security Protocol (IPsec) - network layer security
    - secures IP datagrams between two network-layer entities
    - used to create VPNs (virtual private networks) that run over public Internet
    - provide data integrity, origin authentication, replay attack prevention, confidentiality.
    - Two protocols
        - Authentication Header (AH)
            - provides source authentication and data integrity but not confidentiality.
        - Encapsulation Security Protocol (ESP)
            - provides source authentication, data integrity, and confidentiality, thus more common.
        - IPsec datagram





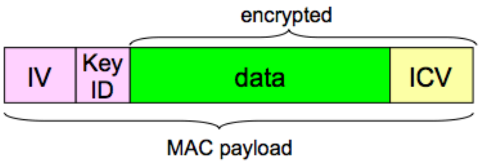
IPsec summary

- IKE message exchange for algorithms, secret keys, SPI numbers
- either AH or ESP protocol (or both)
  - AH provides integrity, source authentication
  - ESP protocol (with AH) additionally provides encryption
- IPsec peers can be two end systems, two routers/ firewalls, or a router/firewall and an end system

- Wired Equivalent Privacy (WEP)
  - an easily broken security algorithm for IEE802.11.
  - uses symmetric key cryptography.
  - self-synchronizing: each packet encrypted separately.
  - uses RC4 symmetric cipher

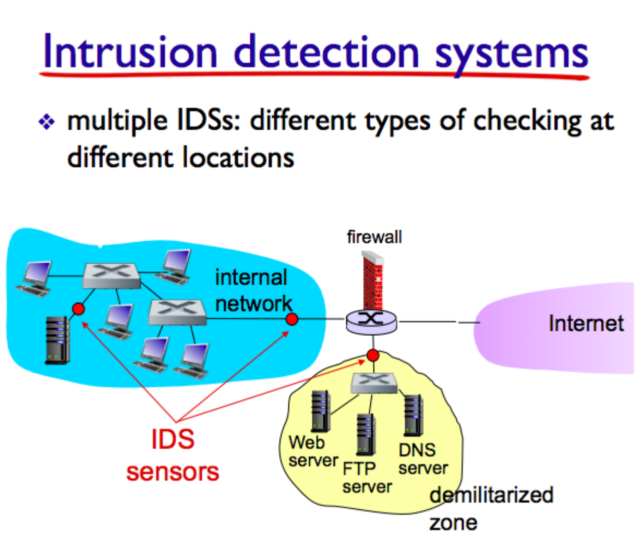
WEP encryption (1)

- 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:
  - B\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



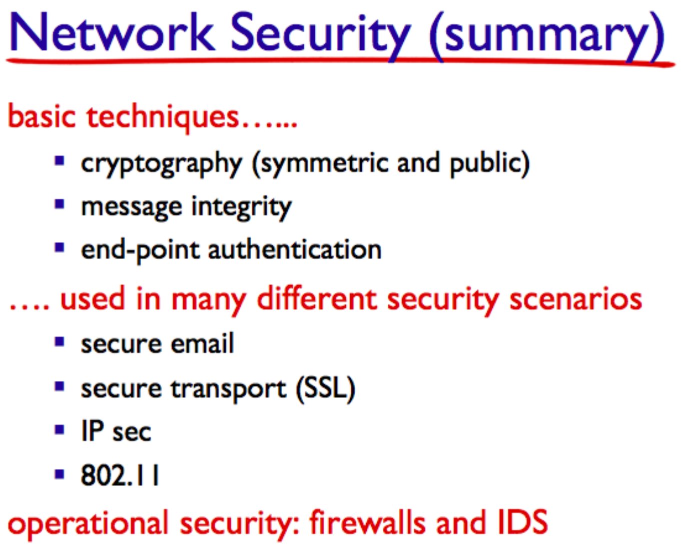
○

    - New initialization vector (IV) for each frame!
- Firewalls
    - isolates organizations internal network from larger Internet, allowing some packets to pass, blocking others.
    - Form of intrusion prevention system.
    - Prevent DoS attacks, illegal modifications/access of internal data.
    - allow only authorized access to internal network.
    - Three types of firewalls: stateless/stateful packet filters and application gateways.
    - Packet filters
        - Stateless
            - internal network separated to Internet via router firewall which filters incoming/outgoing packet-by-packet.
            - Uses Access Control LIsts (ACL) to determine rules. - table of rules, applied top to bottom to incoming packets.
        - Stateful
            - track status of every TCP connection from setup SYN to teardown FIN and determine whether packets “make sense.”
        - App gateways
            - filters packets on application data as well as on IP/TCP/UDP fields
            - 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
    - 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 (SSL)
- IP sec
- 802.11

operational security: firewalls and IDS