EN.601.414/614 Computer Networks

Security

Xin Jin

Spring 2019 (MW 3:00-4:15pm in Shaffer 301)

JOHNS HOPKINS UNIVERSITY

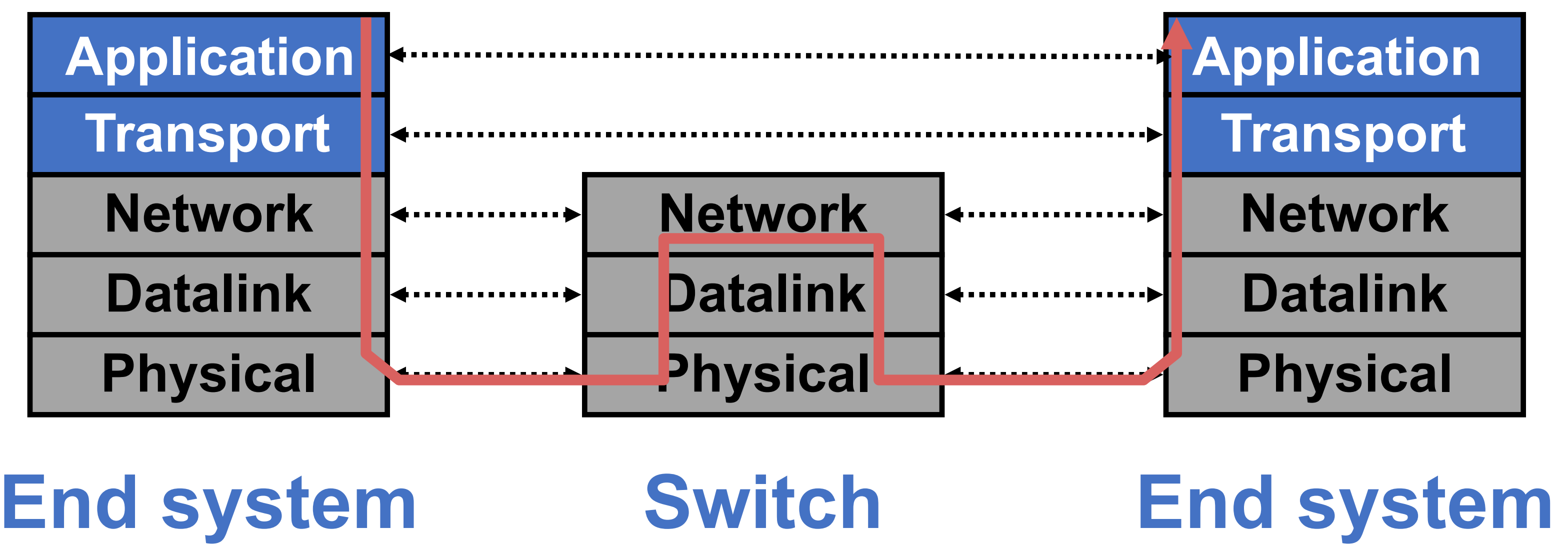
https://github.com/xinjin/course-net

Agenda

- **Common security issues and challenges in the network stack**

Layers in the network stack

- Communication goes down to physical network
- Then up to relevant layer



Layer 7: Too many to cover

- **Layer 7 applications present a wide range of diverse threats**
  - Server-side vulnerabilities (e.g., buffer overflow, SQL injection, XSS), spam, phishing, account theft, …
  - Leading to many cybercrimes
- **Not our focus**

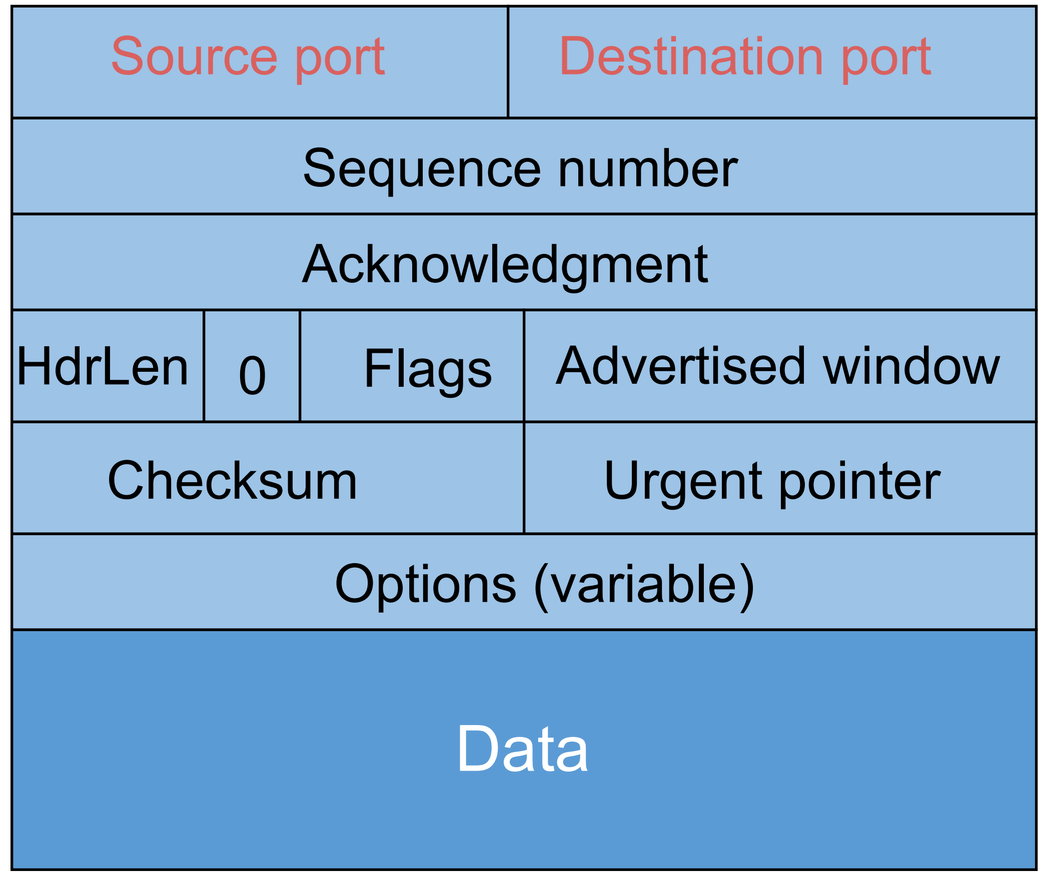
General goals for communication security: CIA

- **Confidentiality**
  - No one read our communication
  - Cryptography
- **Message Integrity**
  - No one can modify our communication w/o detection
  - Verification
- **Availability and Authentication**
  - Redundancy, DoS/DDoS prevention
  - Only we can access our data and communicate on our behalf

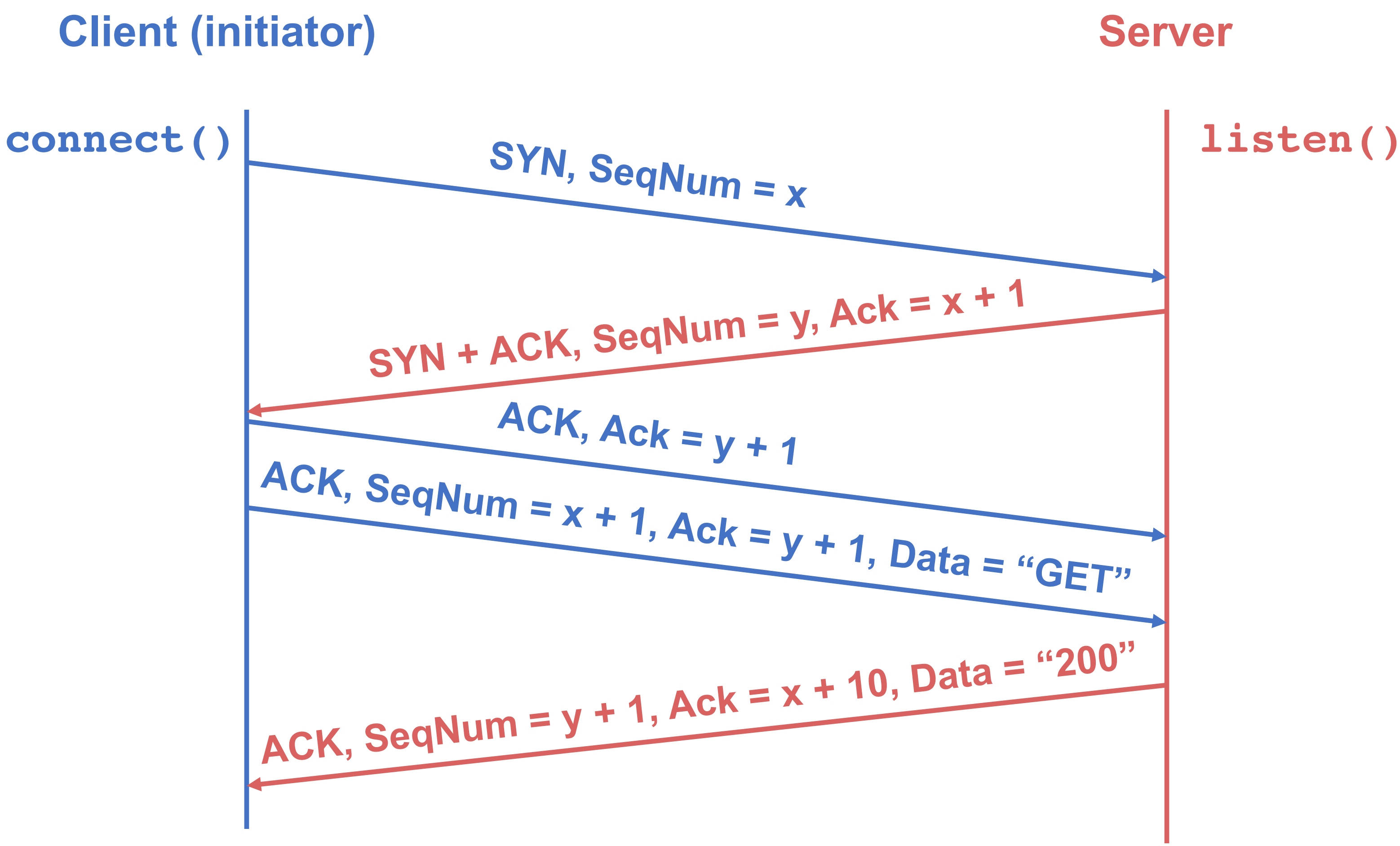
A quick look at TCP

Layer 4: Manipulation of TCP

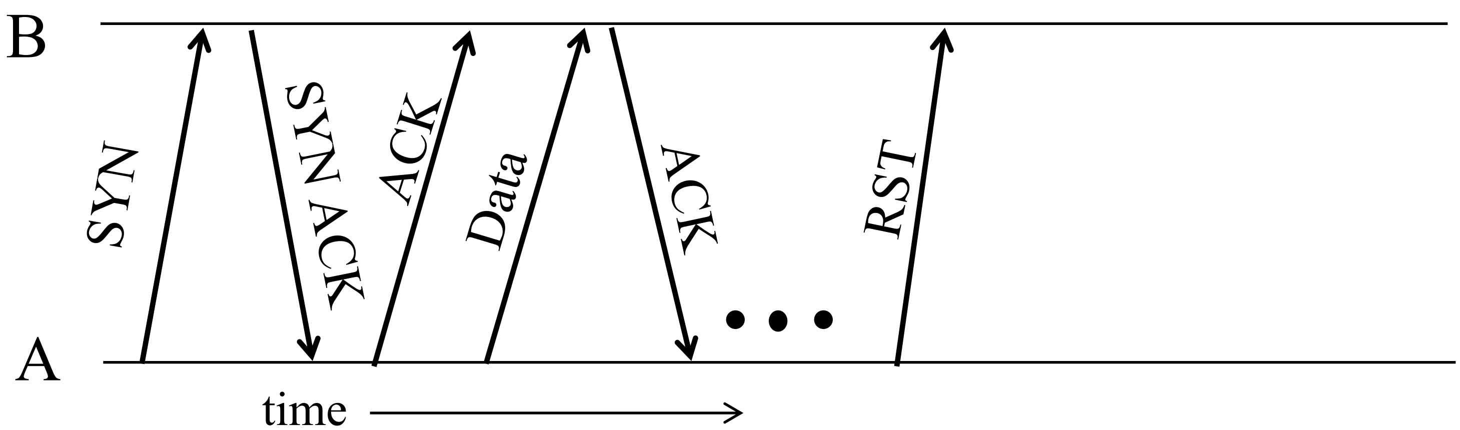
- **Source and destination port/IP define a connection**
- **Sequence number of a packet define its place in the stream**



TCP’s 3-Way handshaking

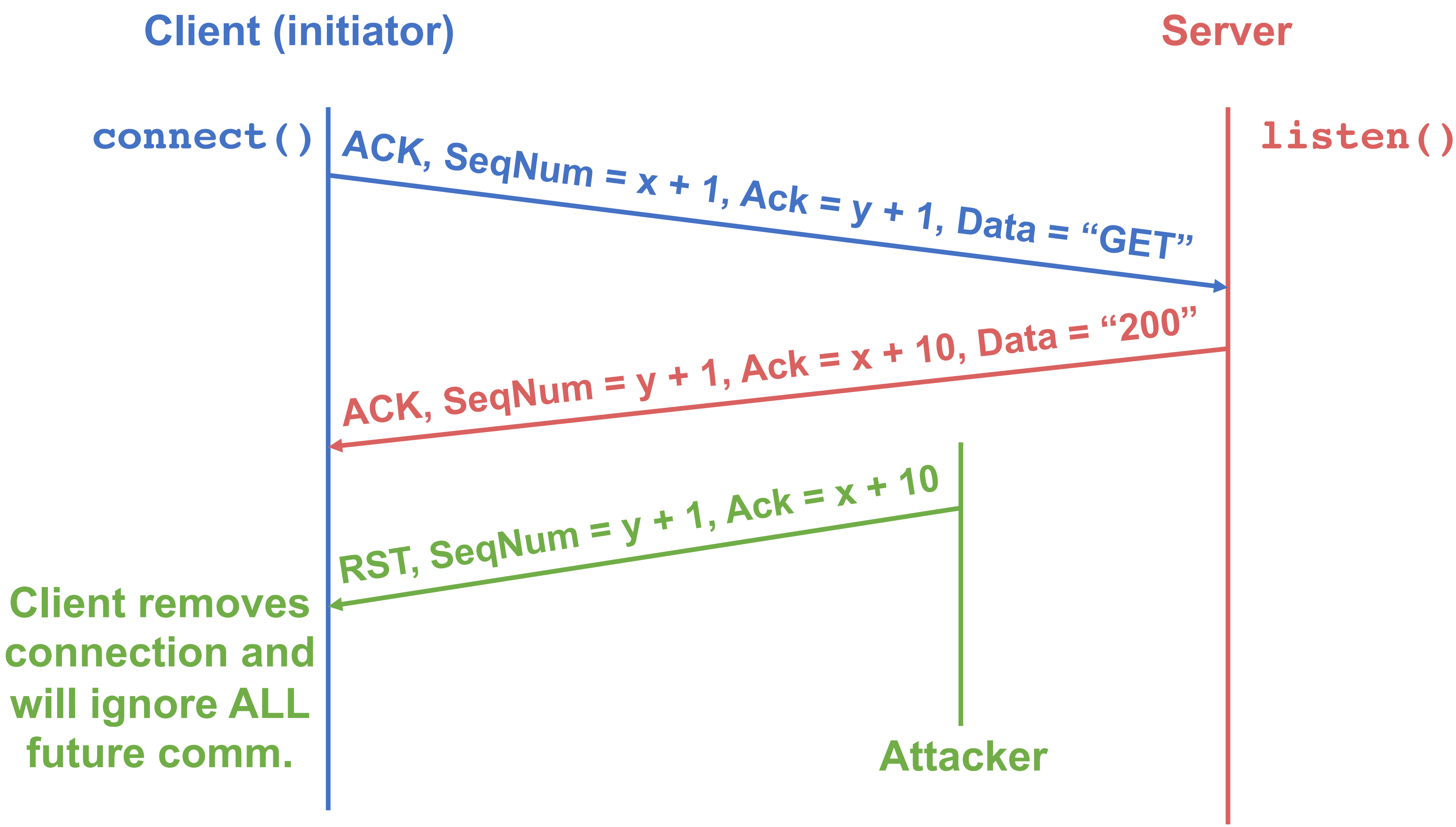


TCP abrupt termination



- **A sends a RESET (RST) to B**
  - E.g., because application process on A crashed
- **That's it**
  - B does not ack the RST
  - Thus, RST is not delivered reliably, and any data in flight is lost
- **An attacker who knows ports and sequence numbers can disrupt any TCP connection**

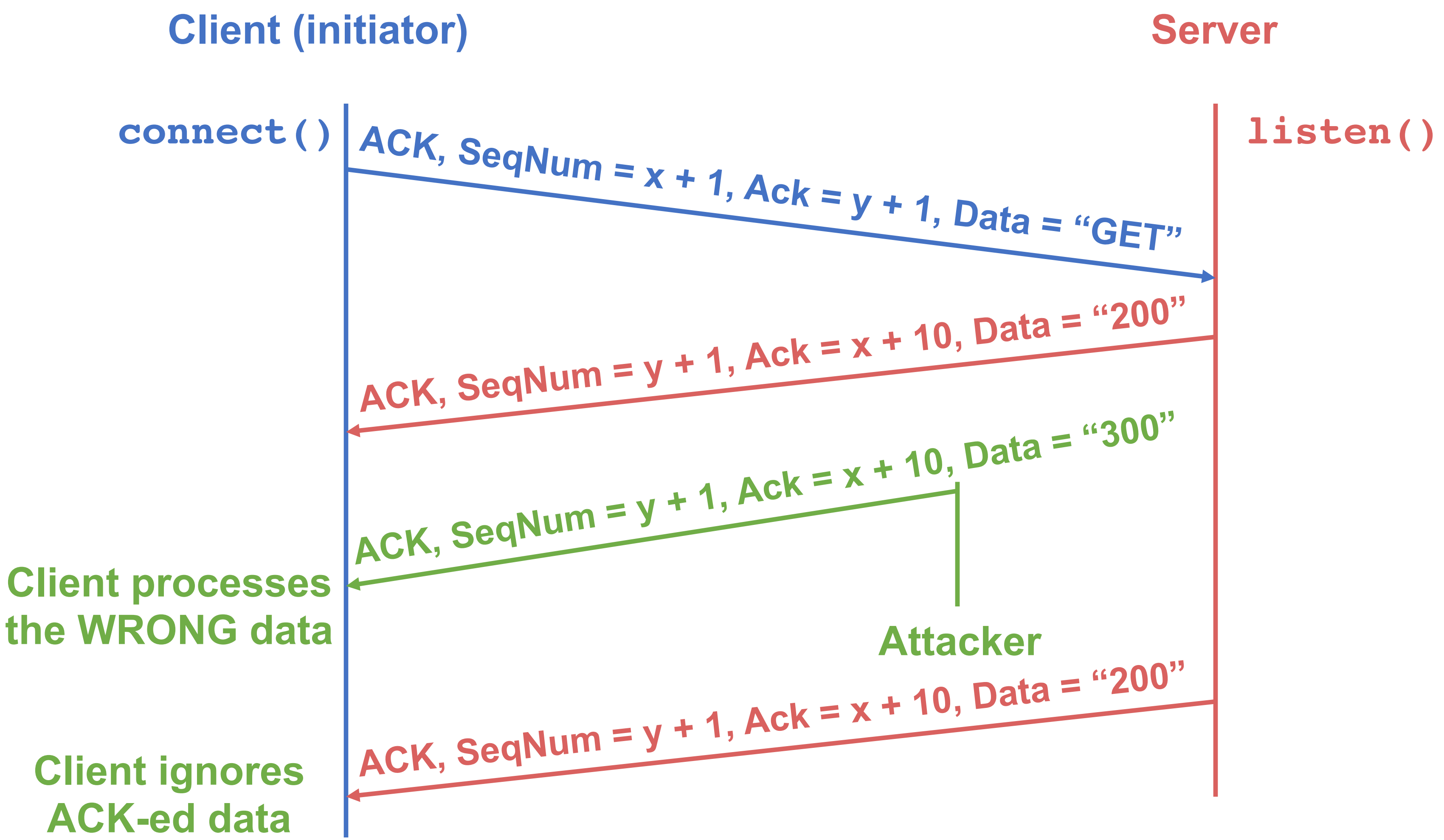
TCP RST injection



Connection hijacking

- **Taking over an already-established connection instead of RST injection**
  - Even worse!

TCP data injection



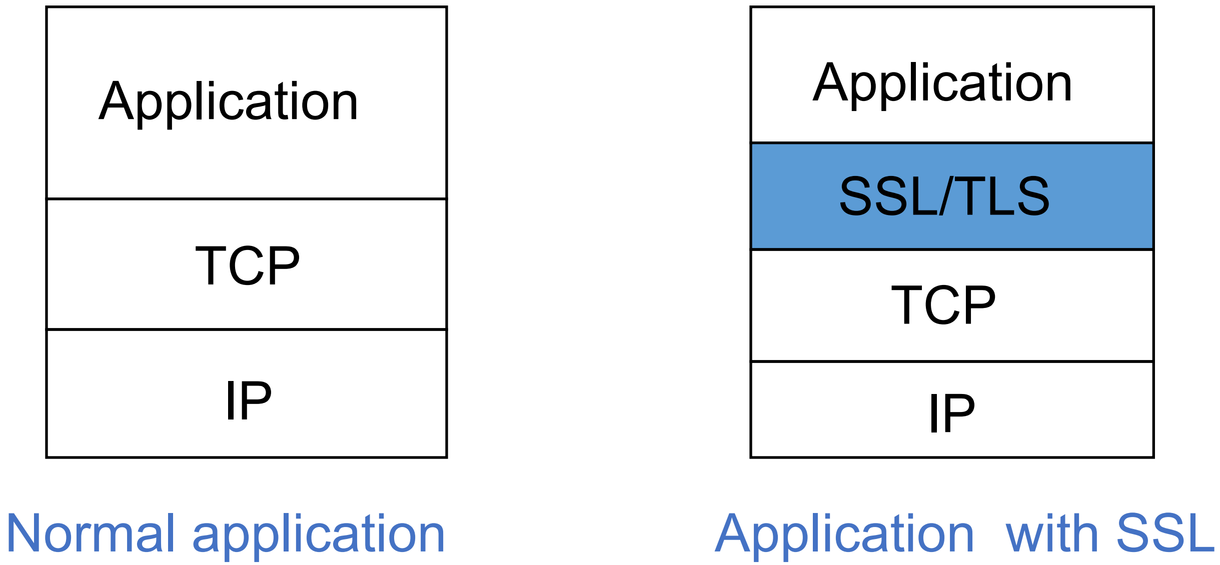
Connection hijacking

- **Taking over an already-established connection instead of RST injection**
  - Even worse!
- **Root cause**
  - Attacker can see packet contents and thus knows port/IP and SeqNum

Secure Sockets Layer (SSL)

- **Transport layer security for TCP-based apps**
- **Used between Web browsers and servers (HTTPS)**
- **Security services:**
  - Server authentication (is it really your bank's server?)
  - Data encryption (transaction not altered)
  - Client authentication (optional)
- **SSLv3 was the ancestor of IETF's Transport Layer Security (TLS)**

SSL/TLS and TCP/IP



- **SSL provides application programming interface (API) to applications**
- **C and Java SSL libraries/classes readily available**

TCP security issues

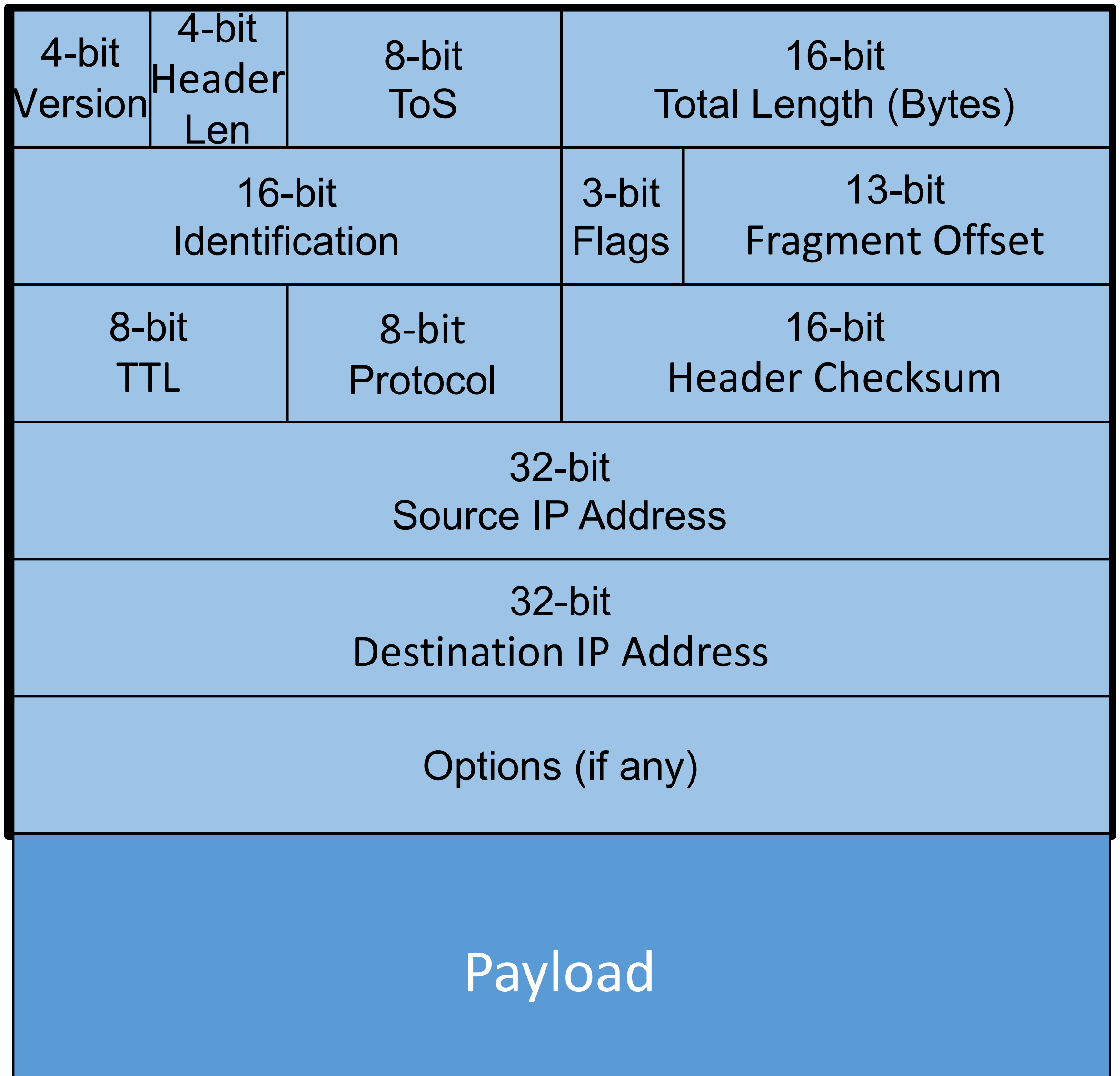
- **An attacker who can observe packets, can**
  - ➢ Forcefully RST connections
  - ➢ Inject forged data
  - ➢ A major challenge today
- **SSL/TLS provide**
  - ➢ Confidentiality
  - ➢ Data integrity
  - ➢ Authentication
- **SSL/TLS can handle data injection but not RST injection**

A quick security analysis of the IP header

Focus on sender attacks

- **Vulnerabilities sender can exploit**
- **Ignore (for now) attacks by others**
    - Traffic analysis
    - Snooping payload
    - Denial of service

IP packet structure



IP address integrity

- **Source address should be the sending host**
  - ➢But, you could send packets with any source you want

Implications of IP address integrity

- **Why would someone use a bogus source address?**
- **Launch a denial-of-service attack**
  - ➢ Send excessive packets to the destination to overload the node, or the links leading to the node
  - ➢ But: victim can identify/filter you by the source address
- **Evade detection by "spoofing"**
  - ➢ Put someone else's source address in the packets
    - Or: use many different ones so can't be filtered

More security implications

- **IP options**
  - Misuse: e.g., Source Route lets sender control path taken through network - say, sidestep security monitoring
  - IP options often processed in router's slow path → attacker can try to overload routers
- **Firewalls often configured to drop packets with options**

Security implications of ToS

- **Attacker sets ToS priority for their traffic**
  - If regular traffic does not set ToS, then network prefers the attack traffic, greatly increasing damage
- **Today, network ToS generally does not work**
  - ToS now redefined for differentiated service
  - Mostly set/used by network operators, not end-systems

Security implications of fragmentation

- **Allows evasion of network monitoring/enforcement**
- **E.g., split an attack across multiple fragments**
  - ➢Packet inspection won't match a "signature"

`Offset=0` `Offset=8`

`Nasty-at`	`tack-bytes`

- **Monitor must remember previous fragments**
  - ➢But that costs state, which is another vector of attack

More fragmentation attacks

- **What happens if attacker doesn't send all of the fragments in a packet?**
- **Receiver (or firewall) winds up holding the ones they receive for a long time**
  - State-holding attack

Security implications of TTL

- **Allows discovery of topology (a la traceroute)**
- **Can provide a hint that a packet is spoofed**
  - ➢ It arrives at a router w/ a TTL different than packets from that address usually have
    - Because path from attacker to router has different # hops
  - ➢ Brittle in the presence of routing changes
- **Initial value is somewhat distinctive to sender's operating system. This plus other such initializations allow OS fingerprinting …**
  - ➢ Which allow attacker to infer its likely vulnerabilities

Other security implications

- **No apparent problems with the protocol field**
  - It's just a de-muxing handle
  - If set incorrectly, next layer will find packet ill-formed
- **Bad IP checksum field will cause packet to be discarded by the network**
  - Not an effective attack

Preventing (some) network layer threats

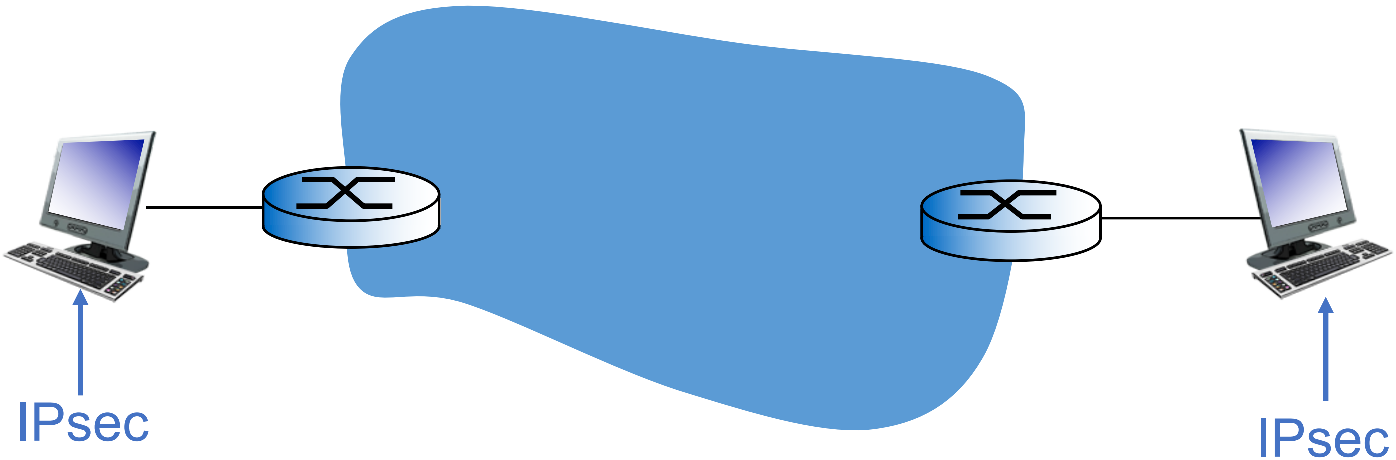
Security at the network layer

- **There are security concerns that apply to multiple applications and cut across protocol layers**
- **Benefits of network-layer security**
  - ➢Below transport layer: transparent to applications
  - ➢Can be transparent to end users
  - ➢Helps secure routing architecture

IPsec: Network layer security

- **Provides**
  - Network-layer authentication: destination host can authenticate source IP address
  - Network-layer confidentiality and integrity:
    - Sending host encrypts the data in IP datagram
- **Two principle protocols:**
  - Authentication header (AH) protocol
  - Encapsulation security payload (ESP) protocol
  - Mandatory in IPv6, optional in IPv4

IPsec transport mode



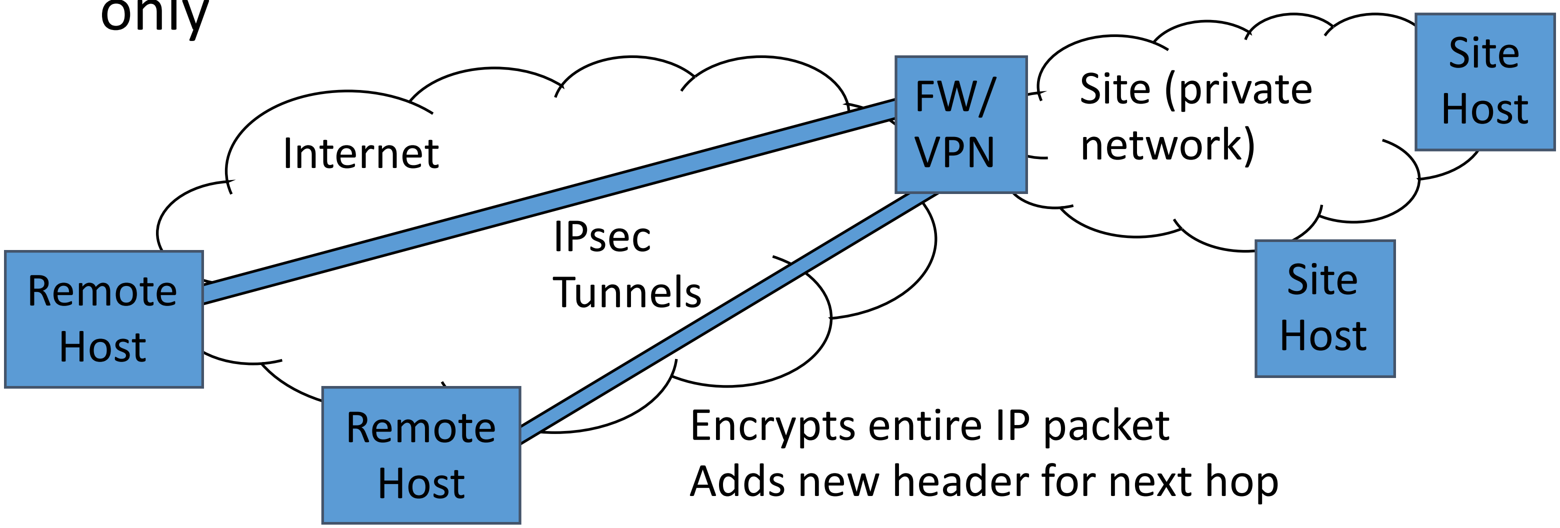
- IPsec datagram emitted and received by end-system
- Protects upper level protocols
- The routers/switches can also be IPsec-aware

Virtual Private Network (VPN)

- **VPN makes separated IP sites look like one private IP network**
    - Private addresses and domain names (useful for authorization)
- **Security via IPsec tunnels**
- **Simplified network operation: ISP can do the routing for you**
- **Building a real private network is expensive (cheaper to use shared resources rather than to have dedicated resources)**

End-to-end VPNs

- **Solves the problem of connecting remote hosts to a firewalled network**
  - ➢Commonly used for roaming
  - ➢Benefits in the form of security and private addresses only



BGP security

Recap: BGP security issues

- **An AS can claim to serve a prefix that they actually don't have a route to**
  - Problem not specific to policy or path vector
  - Important because of AS autonomy
  - Fixable: make ASes "prove" they have a path
- **AS may forward packets along a route different from what is advertised**
  - Tell customers about fictitious short path…
  - Much harder to fix!

Security goals for BGP

- **Secure message exchange between neighbors**
  - Confidential BGP message exchange
  - No denial of service
- **Validity of the routing information**
  - Origin authentication
  - AS path authentication
  - AS path policy
- **Correspondence of the forwarding path**
  - Does the traffic follow the advertised AS path?

Prefix hijacking

- **Another AS originates the prefix**
  - BGP does not verify that the AS is authorized
  - Registries of prefix ownership can be stale and inaccurate
- **Consequences for the affected ASs**
  - Blackhole: Data traffic is discarded
  - Snooping: Data traffic is inspected; then redirected
  - Impersonation: Data traffic is sent to bogus destinations
- **There can also be sub-prefix hijacking**

Hijacking is hard to detect

- **Legitimate origin AS doesn't see the problem**
  - Picks its own route; may not even learn of the bogus
- **May not cause loss of connectivity**
  - E.g., if the bogus AS snoops and redirects
  - May only cause performance degradation
- **Loss of connectivity may be isolated**
  - E.g., only for sources in parts of the Internet

How to diagnose prefix hijacking?

- **Needs many vantage points across the Internet**
  - Analyze updates from many vantage points
  - Launch traceroute from many vantage points
  - Requires access to BGP routers or hosts across the Internet

Feb 24, 2008 YouTube outage (100 minutes – 2 hours)

- **YouTube (AS 36561)**
  - Address block 208.65.152.0/22
- **Pakistan Telecom (AS 17557)**
  - Receives govt. order to block YouTube access
  - Starts announcing 208.65.153.0/24 to its provider PCCW (AS 3491)
  - All packets directed to YouTube get dropped
- **Mistakes were made**
  - AS 17557: Announced to everyone, not just customers
  - AS 3491: Not filtering routes announced by AS 17557

Many other issues

- **BGP session security**
- **AS path validity**
  - ➢Remove, add, or modify ASes in AS path
- **Forwarding issues**
  - ➢Routing does not mean nor control forwarding
- **Overall, BGP today is**
  - ➢Vulnerable
  - ➢Hard to fix (even though we have some solutions like S-BGP and BGPsec)

Physical and link layer issues

Eavesdropping/sniffing

- **For subnets using broadcast technologies (e.g., WiFi, pre-2000 Ethernet), it's free**
- **For any technology, routers/switches transferring the data can look at/capture/export data**

Denial of Service (DoS)

- **Overload/jam signals (e.g., in wireless networks)**
- **Introduce ill-formed frames/packets**
- **Just drop frames/packets**

Spoofing

- **Introduce forged frames/packets**
- **More powerful when combined with eavesdropping**
  - We've seen its examples already in upper layers

DHCP vulnerabilities

- **Attacker can listen to DHCP requests that new host broadcast**
- **Can respond with forged offers before the actual DHCP server**
  - ➢Essentially, taking over DNS, gateway, and other core information, and insert itself as a man-in-the-middle

Summary

- **Ensuring network security is a constant battle**
  - ➢AND, a vast field on its own
  - ➢We just looked at a few random samples

Thanks!
Q&A