

Computer Security

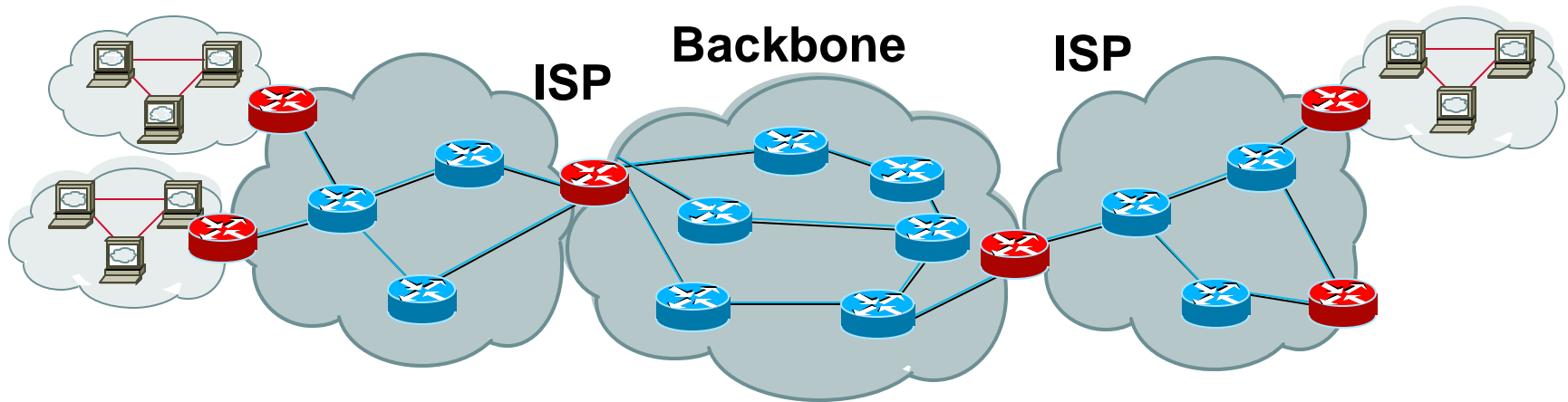
CS 426

Lecture 21

Basic Network Security Problems

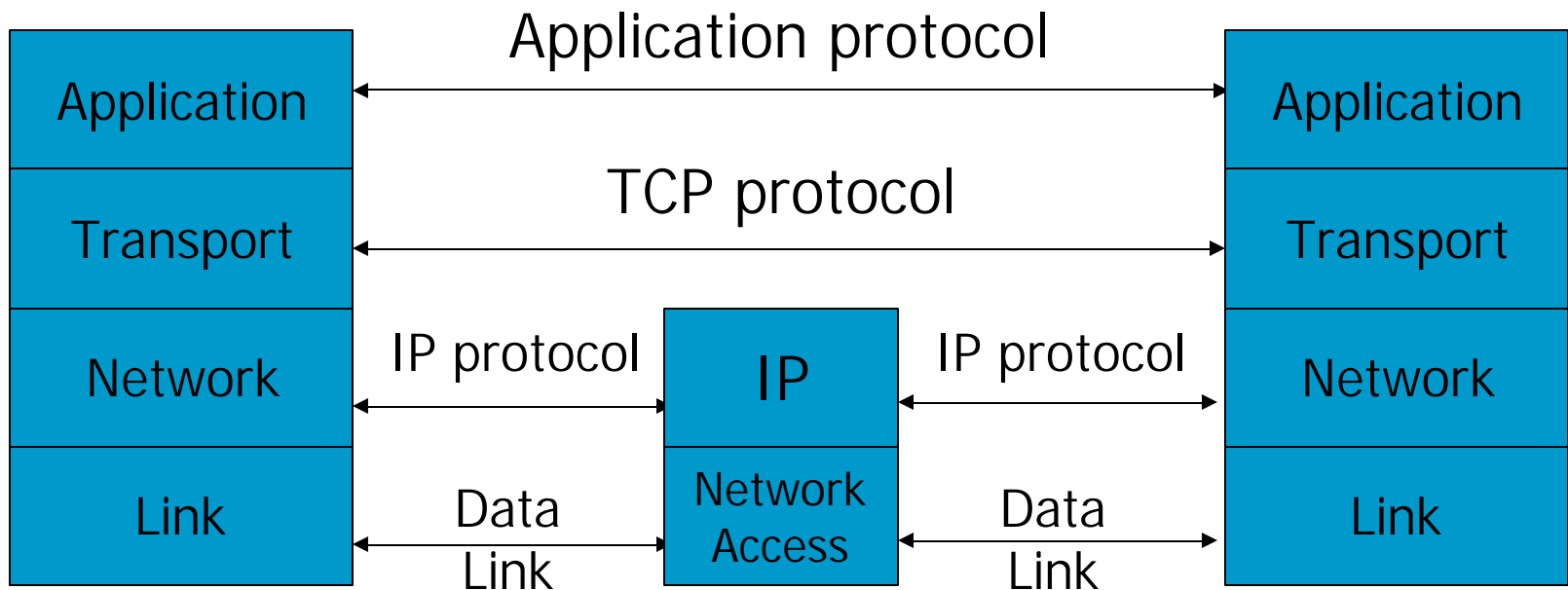
- Required Reading
 - Counter Hack Reloaded: Chapter 2, Networking Overview
 - Counter Hack Reloaded: Chapter 8, Gaining Access Using Network Attacks
- Many slides taken from Prof. John Mitchell's Stanford CS 155 and modified)

Internet Infrastructure



- Local and interdomain routing
 - TCP/IP for routing, connections
 - BGP for routing announcements
- Domain Name System
 - Find IP address from symbolic name

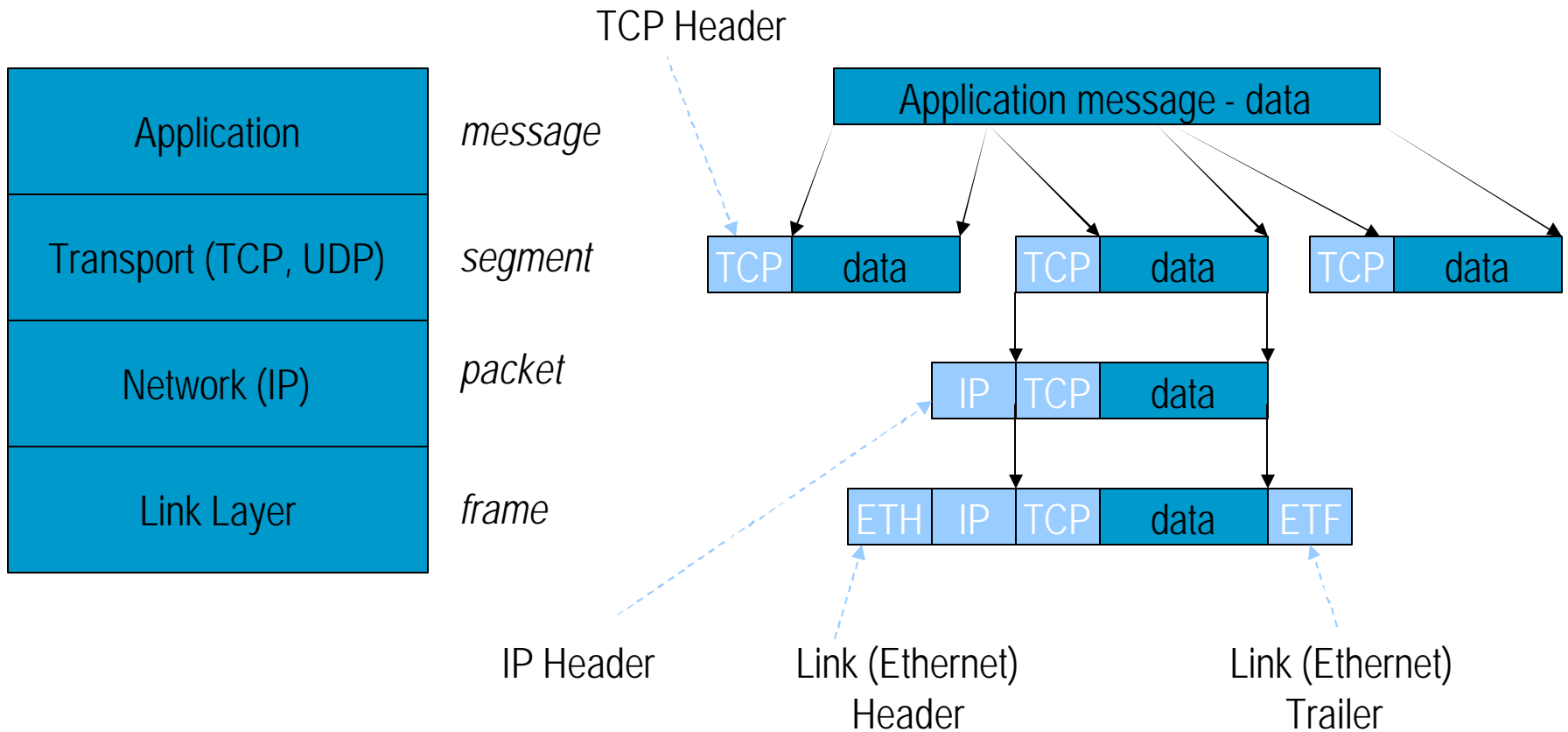
TCP Protocol Stack



Protocols

Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SNMP, SSH, TELNET, ECHO, BitTorrent, RTP, PNRP, rlogin, ENRP
	BGP
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP
Internet	OSPF, ICMP and IGMP
	IP (IPv4, IPv6)
	ARP and RARP
Network access	Ethernet, Wi-Fi, token ring, PPP, SLIP, FDDI, ATM, Frame Relay, SMDS

Data Formats



IP Internet Protocol

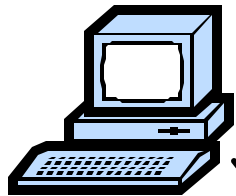
- Connectionless
 - Unreliable
 - Best effort
- Transfer datagram
 - Header
 - Data

Version	Header Length
Type of Service	
Total Length	
Identification	
Flags	Fragment Offset
Time to Live	
Protocol	
Header Checksum	
Source Address of Originating Host	
Destination Address of Target Host	
Options	
Padding	
IP Data	

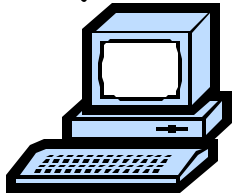
IP Routing



Meg



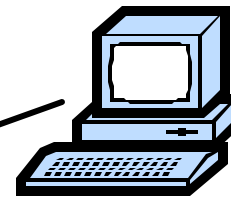
121.42.33.12



ISP

121.42.33.1

Packet	
Source	121.42.33.12
Destination	132.14.11.51
Sequence	5

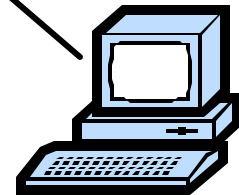


Office gateway

132.14.11.1



Tom



132.14.11.51

- Internet routing uses numeric IP address
- Typical route uses several hops

IP Protocol Functions (Summary)

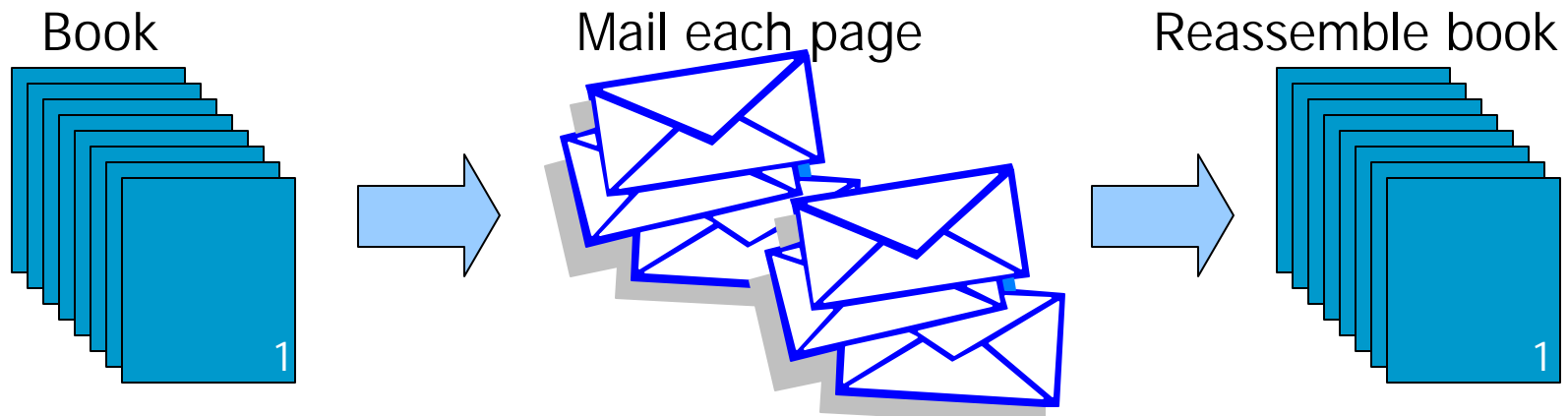
- Routing
 - IP host knows location of router (gateway)
 - IP gateway must know route to other networks
- Fragmentation and reassembly
 - If max-packet-size less than the user-data-size
- Error reporting
 - ICMP packet to source if packet is dropped

User Datagram Protocol

- IP provides routing
 - IP address gets datagram to a specific machine
- UDP separates traffic by port
 - Destination port number gets UDP datagram to particular application process, e.g., 128.3.23.3:53
 - Source port number provides return address
- Minimal guarantees
 - No acknowledgment
 - No flow control
 - No message continuation

Transmission Control Protocol

- Connection-oriented, preserves order
 - Sender
 - Break data into packets
 - Attach packet numbers
 - Receiver
 - Acknowledge receipt; lost packets are resent
 - Reassemble packets in correct order



Internet Control Message Protocol

- Provides feedback about network operation
 - Error reporting
 - Reachability testing
 - Congestion Control
- Example message types
 - Destination unreachable
 - Time-to-live exceeded
 - Parameter problem
 - Redirect to better gateway
 - Echo/echo reply - reachability test
 - Timestamp request/reply - measure transit delay

Address Resolution Protocol (ARP)

- Primarily used to translate IP addresses to Ethernet MAC addresses
- Also used for IP over other LAN technologies, e.g., FDDI, or IEEE 802.11
- Each host maintains a table of IP to MAC addresses
- Message types:
 - ARP request
 - ARP reply
 - ARP announcement

Some Security Problems

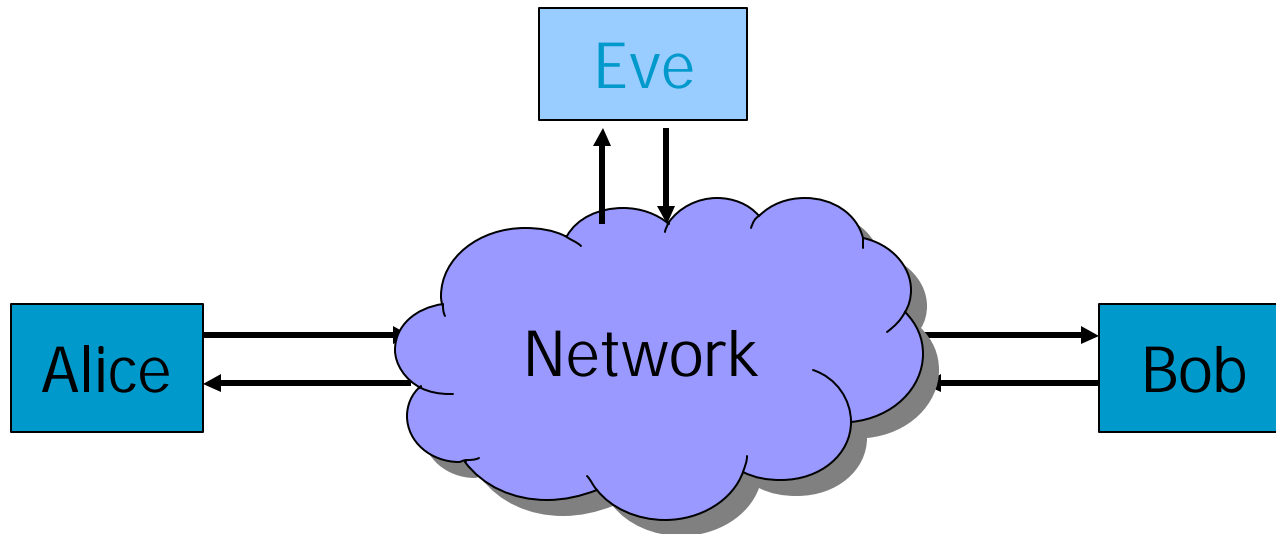
- ARP is not authenticated
 - APR spoofing (or ARP poisoning)
- Network packets pass by untrusted hosts
 - Eavesdropping, packet sniffing (e.g., “ngrep”)
- Session Hijacking Attacks
- TCP state can be easy to guess
 - TCP spoofing attack

ARP Spoofing (ARP Poisoning)

- Send fake or 'spoofed', ARP messages to an Ethernet LAN.
 - To have other machines associate IP addresses with the attacker's MAC
- Defenses
 - static ARP table
 - DHCP Snooping (access control based on IP, MAC, and port)
 - detection: Arpwatch, Reverse ARP
- Legitimate use
 - redirect a user to a registration page before allow usage of the network

Packet Sniffing

- Promiscuous NIC reads all packets
 - Read all unencrypted data (e.g., “ngrep”)
 - ftp, telnet send passwords in clear!



Prevention: Encryption, improved routing (IPSEC)

Tools for Network Sniffing

- tcpdump
- Windump
- Snort (network sniffer and network intrusion detection system)
- Wireshark (formerly Ethereal)
 - history of lot of buffer overflow vulnerabilities
- Sniffiy
- Dsniff

Passive Sniffing and Active Sniffing

- Sniffing through a hub
 - a hub forwards all traffic to all connected ports
 - allows passive sniffing
- Active sniffing through a switch
 - tool: dsniff
 - flooding attacks
 - using ARP spoofing

Session Hijacking Attacks

- Host-based session hijacking
 - if having root privilege, can read and write local terminal devices
- Network-based session hijacking
 - often against TCP

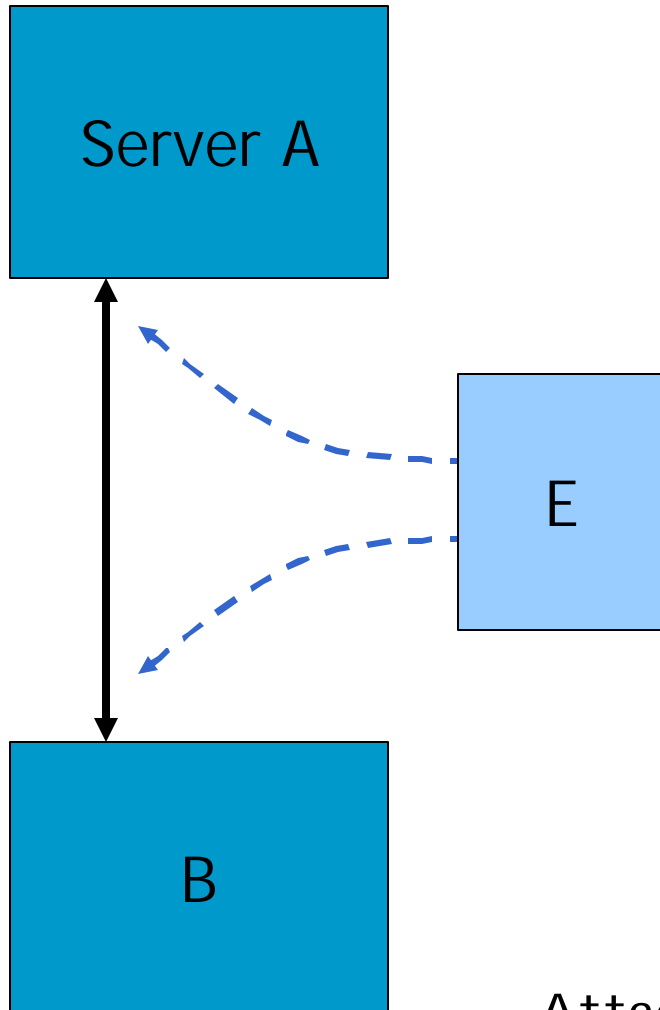
Risks from Session Hijacking

- Inject data into an unencrypted server-to-server traffic, such as an e-mail exchange, DNS zone transfers, etc.
- Inject data into an unencrypted client-to-server traffic, such as ftp file downloads, http responses.
- IP addresses often used for preliminary checks on firewalls or at the service level.
- Hide origin of malicious attacks.
- Carry out MITM attacks on weak cryptographic protocols.
 - often result in warnings to users that get ignored
- Denial of service attacks, such as resetting the connection, can be performed.

TCP Session Hijacking

- Each TCP connection has an associated state
 - Client IP and port number; same for server
 - Sequence numbers for client, server flows
- Problem
 - Easy to guess state
 - Port numbers are standard
 - Sequence numbers often chosen in predictable way

IP Spoofing Attack



- A, B trusted connection
 - Send packets with predictable seq numbers
- E impersonates B to A
 - Opens connection to A to get initial seq number
 - DoS B's queue
 - Sends packets to A that resemble B's transmission
 - E cannot receive, but may execute commands on A

Attack can be blocked if E is outside firewall.

TCP Sequence Numbers

- Need high degree of unpredictability
 - If attacker knows initial seq # and amount of traffic sent, can estimate likely current values
 - Send a flood of packets with likely seq numbers
 - Attacker can inject packets into existing connection
- Some implementations are vulnerable

Recent DoS vulnerability [Watson'04]

- Suppose attacker can guess seq. number for an existing connection:
 - Attacker can send Reset packet to close connection. Results in DoS.
 - Naively, success prob. is $1/2^{32}$ (32-bit seq. #'s).
 - Most systems allow for a large window of acceptable seq. #'s
 - Much higher success probability.
- Attack is most effective against long lived connections, e.g. BGP.

Cryptographic network protection

- Solutions above the transport layer
 - Examples: SSL and SSH
 - Protect against session hijacking and injected data
 - Do not protect against denial-of-service attacks caused by spoofed packets
- Solutions at network layer
 - Use cryptographically random ISNs [RFC 1948]
 - More generally: IPsec
 - Can protect against
 - session hijacking and injection of data
 - denial-of-service attacks using session resets

Summary

- ARP spoofing (ARP poisoning)
 - fixed mapping, access control, or detection
- Eavesdropping
 - Encryption, improved routing
- Session Hijacking
 - Use less predictable sequence numbers

Coming Attractions ...

- November 8:
 - DNS Security and Denial of Service Attacks
- Reading:
 - Counter Hack Reloaded: Chapter 9: Denial-of-Service Attacks

