Computer Networks

-Course review-

College of Information Science and Engineering
Ritsumeikan University

RITSUMEIKAN UNIVERSITY

W14 short test (1)

- The basic function of the Real-time Transport protocol (RTP) is to multiplex several real-time data streams onto a single stream of UDP packets.
- In lossy compression, the decoded output is not exactly equal to the original input.
- In H.323, the gateway connects the Internet to the telephone network.
- What are the two asymmetries of compression systems?
  - The encoding can be slow and require expensive hardware, but the decoding need to be fast and require relatively inexpensive hardware. Also, the decoded output might not be exactly equal to the original input (so it is lossy).

W14 short test (2)

- Explain how DASH works, and what are the differences between DASH and HLS!
  - Dynamic Adaptive Streaming over HTTP: the streaming server first encodes the movies at multiple resolutions and frame rates, and has them stored in many files (each stores few secs of audio and video). The video files are provided by the server according to the bandwidth of the user which is measured periodically to ensure the best possible quality without delay. Apple's proprietary HLS includes some additional features (e.g., fast forward and backward), and doesn't allow ads in the stream.
- In terms of QoS requirements, what is the biggest difference between streaming a movie and Internet telephony?
  - The biggest difference in terms of QoS is the need for low latency for Voice over IP/Internet telephony. This can be quite difficult to achieve, because the maximum tolerable is 150 msecs. Voice over IP systems use short packets (instead of larger packets) to reduce latency at the cost of bandwidth efficiency.

W14 short test (3)

- What are H.323 and SIP, and what is the architectural difference between them?
  - H.323 is a whole protocol suite of Internet telephony: references a large number of protocols for speech coding, call setup, signaling, data transport, etc., in a monolithic architecture. The Session Initiation Protocol describes how to set up Internet telephone calls, video conferences, and other multimedia connections in a modular architecture.

W14 recap (1)

- Security properties: Confidentiality, Integrity, Availability, Authentication, Nonrepudiation
- Attack principles: Reconnaissance, Sniffing, Spoofing, Disruption
  - OSINT, port scanning
  - MAC cloning, ARP spoofing, MITM attack
  - DNS spoofing, TCP spoofing
  - denial-of-service attacks, DDoS
- The firewall acts as a packet filter, as it inspects each and every incoming and outgoing packet
- The role of an IDS is to detect attacks (signature-based or anomaly-based)
- An IPS should detect and stop an attack
- Cryptography is the study of secure communications techniques

W14 recap (2)

- Messages to be encrypted are known as the plaintext, transformed by a function parameterized by a key
- Substitution, transposition, and one-time pad ciphers
- Symmetric key algorithms
  - DES, AES
- In public-key cryptography, the encryption algorithms and its key are public, while the decryption algorithm has a private key
  - RSA
- Symmetric-key and Public-key signatures

Agenda

- Course overview
- Exam

Network architecture (1)

- Much information on the Internet is accessed using a client-server model
- Network protocols often share a common set of design goals: reliability, resource allocation, evolvability, and security
- The Internet is a collection of different networks that use common protocols and provide common services
- Most networks are organized as a stack of layers
- A service is a set of primitives that a layer provides to the above layer
- A protocol is a set of rules governing the format and meaning of the packets exchanged within a layer

Network architecture (2)

- A set of layers and protocols is a network architecture, where a list of protocols used one per layer, is a protocol stack
- The OSI reference model is useful as a model of computer networks
- The TCP/IP reference model is useful for the representation of protocols
- Five layer model to discuss computer networks: Physical, (Data) Link, Network, Transport, Application

Application layer (1)

- Human-readable domain names must be converted to IP addresses with the DNS
- Name resolution is the process of looking up a name a finding an address
- The Internet is divided into top-level domains and many subdomains in a namespace hierarchy, involving non-overlapping zones
- The email architecture consists of two kinds of subsystems: user agents and mail servers/message transfer agents speaking the SMTP
- RFC 5322 is the basic ASCII Internet message format, and MIME is about multimedia extensions to the basic format'
- One of the main protocols used for the final email delivery is IMAP, an improvement over POP3

Application layer (2)

- Webmail is an alternative to IMAP and SMTP for providing email service, using the Web as an interface
- The World Wide Web is a popular architectural framework for accessing linked content all over the Internet
- HTTP/HTTPS is a request-response protocol with different request methods
- Fetching and rendering a static and dynamic pages involves HTTP/HTTPS requests to many servers
- Each page is assigned an URL that is the page's worldwide name with three parts

Network layer (1)

- The network layer is concerned with getting packets from the source to the destination
- Store-and-Forward packet switching: packets or datagrams are injected into the network individually and routed independently of each other then forwarded to the next router until it reaches the destination
- The algorithm that manages the routing tables and makes the routing decisions is called the routing algorithm
- Router processes: forwarding and routing (static or dynamic)
- Congestion happens when too many packets introduce packet delay and loss that degrades performance
- Two main approaches to deal with congestion: increase the resources or decrease the load
- In general, networks do not need to be lossless for reliable file transfer (QoS)

Network layer (2)

- Connecting heterogeneous networks with machines using different protocols in layers raises multiple issues
  - supporting different packet sizes with packet fragmentation
- If the source and destination hosts are on the same type of network but there is a different network between them, tunneling is used
- The IPv4 datagram consist of a header and a body/payload part
- IP addresses have a network portion and host portion
- Prefix length corresponds to a binary mask of 1s in the network portion: subnet mask
- Subnetting is about allowing the block of addresses to be split into several parts for internal use as multiple networks while acting like a single network
- Combining multiple small prefixes into a single, larger prefix is called route aggregation

Network layer (3)

- Using NAT, before the packet exists the customer network and goes to the ISP, the address is translated from internal to a the shared public IP
- Even with efficiently using CIDR and NAT, running out of addresses is a problem
- IPv6 has longer addresses than IPv4, simplified header, better support for options, and generally better security
- The ICMP is used by routers to send operational information and error messages to other addresses
- The ARP is used to identify data link layer addresses associated with an IP address
- Inside its own network, organizations can use their own IGPs, but routing between independently operated networks must be done with the same exterior gateway protocol (BGP for the Internet)
- Using DHCP, the DHCP server automatically assigns an IP address per request

Transport layer (1)

- The transport layer builds on the network layer to provide data transport with a desired level of reliability
- The goal is to provide reliable data-transmission service to users in the application layer, using the services from the network layer
- Segments exchanged by the transport layer are contained in packets which are exchanged by the network layer, while packets are contained in frames exchanged by the data link layer
- The three-way handshake used by TCP involves one peer checking with the other that the connection request is indeed current with a realiable way to release connections
- UDP is a connectionless protocol without flow or congestion control that is useful for many client-server situations (e.g., DNS, multimedia, broadcasting)

Transport layer (2)

- The connection-oriented TCP service is obtained by both the sender and the receiver creating endpoints called sockets
- Sockets have socket addresses including the IP address of the host and a number local to the host called a port
- The TCP header includes source port and destination port, sequence number, acknowledgment number, TCP header length, eight 1-bit fields, window size, checksum, urgent pointer, options, and data
- Establishing a TCP connection involves multiple connection states and managing the TCP window for the receiver's buffer
- TCP plays the main role in controlling congestion and ensuring reliable transport using a congestion window and algorithms like slow-start

Data link layer (1)

- The data link layer uses the services of the physical layer below it to send and receive bits over communication channels
- Communication channels make errors occasionally, data may be lost
- The data link layer takes the packets it gets from the network layer and encapsulates them info frames for transmission
  1. Provides a well-defined service interface to the network layer
  2. Involves framing sequences of bytes as self-contained segments
  3. Detecting and correcting transmission errors
  4. Regulating the flow of data
- Three main types of possible services: unacknowledged, acknowledged connectionless, acknowledged connection-oriented
- To provide a service to the network layer, the link layer must use the service provided to it by the physical layer

Data link layer (2)

- Methods for breaking up the bit stream into discrete frames: byte count, flag bytes with byte stuffing or bit stuffing, and invalid characters
- FEC include enough redundant information to enable the receiver to deduce what the transmitted data must have been (e.g., Hamming codes)
- Error-detecting codes include only enough redundancy to allow the receiver to deduce that an error has occurred (but not which error) and have it request a retransmission
- PPP is about establishing a direct connection between two nodes without any host or any other networking device in between over many types of physical networks

Ethernet, LAN (1)

- LAN is a private network that operates within and nearby a single building
- In any broadcast network, they key issue involves determining who gets to use the channel when there is "competition" for it
- The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called MAC
- Allocate a single broadcast channel among users: static vs. dynamic allocation
- Many solutions for allocating multiple access channels exist; CSMA/CD
- Classic vs. Switched Ethernet to deal with the increased load
- Switches only output frames to the ports for which those frames are destined: when a switch port receives an Ethernet frame from a station, the switch checks the Ethernet addresses to see which port the frame is destined for

Ethernet, LAN (2)

- Fast, Gigabit, 10+ Gigabit Ethernet standards
- Different devices in different layers: repeater, hub, bridge, switch, router, transport gateway, application gateway
- The Ethernet header was changed to contain a VLAN tag, for logically configured LANs
- Which VLANs are accessible via which ports: configuration tables have to be set up in the bridges

Cable networks, WAN (1)

- Access networks connect subscribers to service providers, and a WAN spans a large geographical area
- When distances are large, network designers must rely on the existing telecommunication facilities
- Three major components in the telephone system: local loops, trunks, and switching offices
- Early DSL technologies over the PSTN were slow, but modern broadband services such as ADSL are high bandwidth
- Common to use variations of FTTX, because the speed of last-mile networks is often constrained by the copper cables used in conventional telephone networks
- Many people nowadays get their television, telephone, and Internet service "over cable"
- A system with fiber for the long-hauls and coaxial cable to the houses is an HFC (Hybrid Fiber Coax), where a single fiber node can feed multiple coaxial cables

Cable networks, WAN (2)

- Same trend with cable and telephone networks: moving fiber closer to the subscriber home, and all access network technologies now use fiber in the backbone
- Although they differ on the last-mile access technology, comparable services and prices
- IPsec is a network protocol suite that authenticates and encrypts the packets of data sent over a network
  - the connection in IPsec between two endpoints having a security identifier is a SA
  - transport and tunnel mode
- VPNs are usually built over the Internet, but without giving up most of the security advantages of a real private network
  - if IPsec is used for tunneling, it is possible to aggregate all traffic between any two pars of offices onto a single authenticated and encrypted SA

Physical layer (1)

- The physical layer defines the electrical, timing, and other interfaces by which bits are sent as signals over channels
- Full-duplex vs. half-duplex vs. simplex links
- Transmission media that rely on a physical cable/wire are often called guided transmission media
  - each type has its own set of trade-offs: frequency, bandwidth, delay, cost, maintenance
- Twisted par has a low cost, and bandwidth depends on the thickness of the wire and the distance traveled
- Coaxial cable has better shielding and greater bandwidth than UTP

Physical layer (2)

- Fiber optics has a huge bandwidth and other advantages, and used for long-haul transmission in network backbones, high-speed LANs, and high-speed Internet access
  - three key components: light source, transmission medium, detector
  - multimode vs single-mode fiber, with two kinds of light sources
  - connectors, splicing, fusing
  - can handle much higher bandwidths than copper, and not affected by as many environmental issues
  - thin and lightweight, but can be damaged easily
  - unidirectional and the interfaces cost more than electrical
- The process of converting between bits and signals that represent them is called digital modulation
  - baseband vs. passband transmission
- When channels are shared by multiple signals it is called multiplexing

Mobile and wireless networks (1)

- The mobile phone system is used for wide area voice and data communication
- In mobile phone systems, a geographic region is divided up into cells
- At the center of each cell is a base station to which all the telephones in the cell transmit
- 1G technology: analog voice, 2G technology: digital voice + GSM standard
- Data traffic began to exceed voice traffic on the fixed network
  - 3G: digital voice and data, 4G is a completely packet-switched network technology
  - even higher data rates and lower latency for 5G by improving the area capacity
- The main wireless LAN standard for over two decades has been the 802.11 (infrastructure and ad hoc modes)

Mobile and wireless networks (2)

- For wireless, the data link layer is split into two or more sublayers
  - the MAC sublayer determines how the channel is allocated
  - the logical link control sublayer's job is to unify the different 802 variants for the network layer
- All of the 802.11 techniques use short-range radios to transmit signals in either the 2.4GHz or the 5GHz frequency bands
- 802.11 tries to avoid collisions with CSMA/CA, and solve the hidden and exposed terminal problem using the NAV field in each frame
- Stations must also authenticate before they can send frames via the AP (nowadays mostly WPA2)

Multimedia communication, streaming (1)

- Real-time audio and video must be played out at some predetermined rate to be useful (different from normal Web traffic)
- There is enough bandwidth, but the key issue for streaming applications is network delay
- Audio is usually compressed to reduce bandwidth needs and transfer times (lossy vs lossless encoding and decoding)
- Audio compression can be done in two ways: waveform coding and perceptual coding
- Worldwide standard for video compression comes from the MPEG, using the JPEG algorithm and three different kind of frames

Multimedia communication, streaming (2)

- A media player designed for streaming is needed: manage user interface, decrypt file, handle transmission errors, decompress content, eliminate jitter
- Dealing with errors depends on whether a TCP-based transport like HTTP is used or UDP-based like RTP
- Streaming using DASH: the streaming server first encodes the movies at multiple resolutions and frame rates, and has them stored in many files
- Biggest difference streaming a movie and Voice over IP/Internet telephony is the need for low latency that is difficult to achieve
- Internet conferencing systems using H.323 and SIP

Basics of network security

- Security properties: Confidentiality, Integrity, Availability, Authentication, Nonrepudiation
- Attack principles: Reconnaissance, Sniffing, Spoofing, Disruption
  - OSINT, port scanning
  - MAC cloning, ARP spoofing, MITM attack
  - DNS spoofing, TCP spoofing
  - denial-of-service attacks, DDoS
- The firewall acts as a packet filter, as it inspects each and every incoming and outgoing packet
- Cryptography is the study of secure communications techniques
- Messages to be encrypted are known as the plaintext, transformed by a function parameterized by a key
  - symmetric key vs. public key algorithms

General info

- Carefully read the announcement about the examination date/time and place
- If you have covid, need to quarantine, etc. contact the office and inform them about your situation and do not come to the exam
- 60 mins written examination, giving up to 60% of your grade
- You are not allowed to bring in additional items (e.g., notes, textbook, etc.)

Type of questions/problems

- *Multi-line answer type* (e.g., Explain the process of the three-way handshake.)
- *Complete the sentence type* (e.g., Transport mode and _____ mode are the two main modes of IPsec.)
- *Matching type* (e.g., Match the units with the layers.)
- *True or False type* (e.g., Broadcasting an Access Point's SSID is not optional. True or False?)

Tips for preparation

- Go through the short tests (you have all the questions and answers for the short tests)
- Make sure you understand the order of layers, and what units and devices are associated with them
- Make sure you can explain store-and-forward packet switching, the DNS lookup process, how switches work, how NAT works, the three-way handshake, similarities and differences between IPv4 and IPv6, types of channel allocation, difference between error correction and detection, what is a VPN, how firewalls work, how symmetric key cryptography works, types of packet fragmentation