CSC 265

9/19/17

Notes 1

Presentation can be saved on laptop, or submitted to blackboard.

**Network Layer:**

Network layer exists in all kinds of devices, packet sent from one device to another device, with many routers in between. Network layer does not have a switch in between. All devices are host/routers. Packet in the host is encapsulated into datagram in network layer, then passes through network through different routers. From destination the package is extracted to top application layer. One of the most important questions is how the package is transported from one host to another host, what is it’s destination and which path does it go?

**Forwarding**, moves packets from router’s input to appropriate router output

**Routing**: determine route taken by packets from source to dest.

Routing algorithm determines end-end path through network, forwarding table determines local forwarding at this router

Network Service Model:

What service model for “channel” transporting datagrams from sender to receiver?

Time-boundary guarantee: is when data is guaranteed to come within a certain time limit.

**Network vs transport layer connection service:**

Network: between two hosts(may also involve intervening routers in case of VCs)

VC = Virtual Circuit

Transport: between two processes

CBR = constant bit rate

VBR = variable bit rate

ABR =

UBR = Unknown bit rate

Virtual Circuits

1. Path from source to destination
2. VC numbers, one number for each link in the path

**Datagram networks:**

No call setup at network layer

Routers: no state about end to end connections(no network-level concept of “connection”)

Packets forwarded using destination host address

Internet(datagram) system is preferred since it is faster, no strict time requirements so its flexible. Different link types. Allows error recovery.

**Router Architecture overview:**

Two key functions:

Run routing algorithms/protocol (RIP = Router Input Port, OSPF =, BGP)

Forwarding datagrams from incoming to outgoing link

Input Port Functions:

Physical Layer has bit-level reception

Data link layer:

e.g. ethernet

Decentralized switching:

Given datagram dest. Lookup output port using forwarding table in input port memory(“match plus action”)

Goal: complete input port processing at ‘line speed’

Queueing if datagrams arrive faster than forwarding rate into switch fabric

Longest Prefix Matching:

When looking for forwarding table entry for given destination address, use longest address prefix that matches destination address

Switching fabrics

Transfer packet from input buffer to appropriate output buffer

Switching rate: the rate at which packets can be transferred from inputs to outputs

Switching via a bus

Datagram from input port memory to output port memory via a shared bus

Bus contention switching speed limited by bus bandwidth

Switching by interconnection network:

Overcome bus bandwidth limitations

Banyan networks, crossbar, other interconnection nets initially developed to connect processors in multiprocessor

Advanced design fragmenting datagram into fixes length cells, switch cells through the0 fabric

Output ports:

Buffering required when datagrams arrive from fabric faster than the transmission rate

Scheduling discipline chooses among queued datagrams for transmission

Datagram(packets) can be lost due to congestion, lack of buffers

Priority Scheduling - who gets best performance, network neutrality

Output port queuing:

Buffering when arrival rate via switch exceeds output line speed

Queuing (delay) and loss can be …

Input port queueing:

Fabric slower than input ports combined -> queueing may …

**Internet Network Layer:**

Slide 30 Week 3 IP Datagram format /Insert the slide as a picture

**IP Fragmentation, Reassembly**:

Network links have Maximum transfer size(MTU) – largest possible link-level frame

Different link types, different MTUs

Large IP datagram divided (“fragmented”) within net

One datagram becomes several datagrams

“Reassembled” only at final destination

IP header bits used to identify, order related fragments

Slide 32 Week 3 Has a good picture of IP Fragmentation

Offset = (total bytes per datagram)/8

**IP Addressing: Introduction**

IP address: 32-bit identifier for host, router interface

Interface: connection between host/router and physical link

Router’s typically have…

**Subnets**

IP Address:

Subnet part – high order bits

Host part – low order bits

What is a subnet?

Device interfaces with same subnet part of IP address

Can physically reach each other without intervening router

Recipe

To determine the subnets, detach each interface from its host or router, creating islands of isolated networks

Each isolated network is called a subnet

**Notes 9/26/17**

IP address – 32bit integer

192.168.0.1 = 11000000 10101000 00000000(represents network address)| 00000001(Host address)

class A is first 8 bits = 11000000 which is 2^24 size

Class B is first 16bits = 11000000 10101000 which is 2^16 size

Class C is first 24bits = 11000000 10101000 00000000 which is 2^8 = 256bit size

Class D is first 32bits = 11000000 10101000 00000000 00000001

192.168.0.1/24

mask – 255.255.255.0 = 11111111 11111111 11111111 00000000

11000000 10101000 00000000 00000001

+ 11111111 11111111 11111111 00000000

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

= 11000000 10101000 00000000 00000000

The address ending in 0 and 255 are reserved thus, hosts can have 254 possible addresses

192.168.0.3/24 and 192.168.0.4/24 are in the same subnet

If you had 192.168.0.1/22(This number determines the size of the network address

Means 11000000 10101000 000000(Network address max of 252 address)|00 00000001

**Practice**: Are these IP addresses in the same subnet?

1) 192.168.34.5/18 = 11000000 10101000 00|100010 00000101 = 192.168.0.0/18 network address 2^14(32-18 = 14)

2) 192.168.48.7/18 = 11000000 10101000 00|110000 00000111 = 192.168.0.0/18 network address

3) 192.168.168.10/18 = 11000000 10101000 10|101000 00001010 = 192.168.128.0/18 (128 because we have a 10 at end of network address and 10000000 is 128) network address

192.168.168.10/18 = mask of 255.255.192.0 = 11111111 11111111 11000000 00000000

11000000 10101000 10000000 00000000 = 192.168.128.0 mask of 255.255.192.0

1 and 2 are in same subnet

Are these IP addresses in the same subnet? Yes

203.203.200.10/20 = 11001011 11001011 1100|1000 00001010

203.203.202.2/20 = 11001011 11001011 1100|1010 00000010

How about with /24 No

11001011 11001011 11001000| 00001010

11001011 11001011 11001010| 00000010

**IP Addressing: Introduction**

Whats a subnet?

Device interfaces with …

With Dynamic Host Configuration Protocol(DHCP) you get a IP address from the server, without needing to do anything specifically.

Notes 2

9/21/17

IP Datagram

Size:4000 bytes

MTU: 700b

Notes 9/28/17

This and next one are the same222.10.237.5/20 11011110 00001010 1111|1111 00000000

222.10.225.6/20 11011110 00001010 1111|

This is different subnet 222.10.223.6/20 11011110 00001010 1101|

Since many Internal IP addresses share the same type, you use an external IP address for any traffic outside of the local network.

A Network Address Translation table is used to translate the messages to external IP address from internal, and making sure messages from outside go to the correct Internal IP address

X to Y is 2

X to Z is 7

Z to Y is 1

|  |  |  |  |
| --- | --- | --- | --- |
| X | X | Y | Z |
| X | 0 | 2 | 7 |
| Y | Inf | Inf | Inf |
| Z | Inf | Inf | inf |

|  |  |  |  |
| --- | --- | --- | --- |
| Y | X | Y | Z |
| X | Inf | Inf | inf |
| Y | 2 | 0 | 1 |
| Z | Inf | Inf | inf |

|  |  |  |  |
| --- | --- | --- | --- |
| Z | X | Y | Z |
| X | Inf | Inf | inf |
| Y | Inf | Inf | Inf |
| Z | 7 | 1 | 0 |

After that then each chart talks to each other and updates, then they update for shortest path for each letter row only for the three charts, then after it updates again.

Notes 10/3/17

Without Border Gateway Protocol(BGP) then there would not be inter-AS routing. This is the protocol that connects all different networks all different ASes.

externalBGP obtains subnet reachability information from neighboring Ases

internalBGP propagate reachability information to all As internal routers

BGP messages:

OPEN

UPDATE

KEEPALIVE

…

Software Defined Network(SDN)

Quiz 1 answers

1. Receiver
2. Don’t take 20 off the max, 3379
3. 255.255.255.240
4. 11011111 00000001 00000011 00011011
5. IPv4 is running out of addresses, IPv4 32 bit, IPv6 128. IPv4 supports fragmentation IPv6 does not. IPv6 does not have checksum

Notes 10/5/17

Transport Layer:

UPD only uses source and destination port, to determine where to send the packet

TCP uses all 4 tuples:

Source IP address

Source port number

Destination IP address

Destination port number

Notes 10/10/17

Lab assignment 3 due 10/27/17

Can write your own traceroute program using ping

Correctness, integrity and order are important for the guaranteed/reliable data transfer(rdt)

Finite State Machine(FSM), subset of the Turing Machine/Simplified version of it. But can be used to solve various problems. A key use case of this in our compilers, all Object Orientated languages(Java etc.) are based on FSM. Transitions from state to state depending upon the event which then triggers an action.

For rdt errors

Acknowledgements: reciever explicitly tells sender that package received ok

Negative acknowlegdements: reciever tells sender that package had errors

If ACK/NAK is corrupted then use a sequence number with each packet that constantly resends the packet until the ACK signal is received. Sequence numbers are 0 and 1, they are sufficient for all packet traffic.

If there is packet loss due to d/c etc. Then the sender waits a “reasonable” amount of time for ACK, if it doesn’t receive it then it will retransmit the packet. This “time out” method requires a countdown timer. Even though the retransmission is a duplicate the sequence number will still cover duplicate packets.

Instead of sending one packet at a time, instead send multiple at the same time.

Notes 10/12/17

Selective repeat dilemma, if you move over without checking then you will have the problem that your packet will send say 0 when the first 0 may have been lost. Your window size cannot be greater than the number of sequence, instead use half of the sequence size.

**TCP**

This protocol is based on packet selective size. TCP is point-to-point which means one sender, one receiver. MSS(Maximum segment size) is like the MTU of Networks but for TCP. MSS is usually 1460 bytes. TCP is a connection-orientated protocol, connection occurs first, then data transfer happens. TCP segment structure is similar to IP structure.

Sequence numbers, byte stream “number” of first byte in segment’s data.

Acknowledgements: seq# of next byte expected from other size

Cumulative ACK

How receiver handles out-of-order segments? TCP spec doesn’t say, it is up to implementor.

TCP generates its first sequence number randomly, because TCP may lose connection between peers, randomly generating sequence numbers avoid the issue of another connection using that sequence number and confusing it with a different host.

TCP uses cumulative ack which means it must get ack from a sequence number before progressing.

Since TCP is duplex, both are hosts and receivers, they can send and receive data from each other, bidirectional activity.

TCP uses Round Trip Time, timeout: Longer than RTT, but RTT varies

They sample the round trip time from sender to receiver then they record the time of the package being sent once, then take the weighted average of those times

TCP provides a service called Flow Control, this is a mechanism to tell the sender when to send the data and how much

TCP can fast retransmit, since the time-out period is often relatively long:

-Long delay before resending lost packets

Detect lost segments via duplicate ACKs

-Sender often sends many segments back-to-back, if segment is lost, there will likely be many duplicate ACKs. Generally 3 duplicates indicates a problem

TCP generally buffers the data when transmitted until it receives the missing parts.

TCP uses threeway handshake

**Notes 10/17**

2-way handshake has 2 major problems, since establishing connection can take some time, if the client terminates their connection the data is still transferred for a bit which might cause problems. One solution is to take client information(port number IP address and a secret number only known by server) it will then know the sequence number, this way if client doesn’t respond, there won’t be any harm to the server since it wont allocate any ports or resources unless it receives an acknowledgement from client.

3-way handshake has both client and server send sequence numbers to each other, then client sends acknowledgement back to server. Each side must close the connection, client sends finish bit and seq # then server sends ack and finish bit and seq # then client sends back acknowledgement

TCP also has congestion control, similar to flow control.

Summary:

Transport layer has 2 important protocols UDP and TCP. The major difference between them is reliability. UDP does not provide guarantees, just wraps data and send it out. TCP however has many different ways of ensuring data arrives where it needs to. UDP has 8 byte overhead header. TCP has 20 byte overhead.

TCP starts with 1500 MTU has 20 header, then 20 overhead so it starts with 1460 usable bytes.

(2^16) – 1 is total number of ports available

SYN is used to establish a connection

**Application Layer**:

Almost all applications are network applications, most use the internet in some function. All the different applications have their own protocols. For all applications you develop the protocols that your software will understand the data being sent.

**Client-server**, always on server providing services, client connects when they want to get the data.

Server has permanent IP address, and has data center for scalability

Clients, communicate with server, may have dynamic IP Addresses, do not communicate directly with each other.

**Peer-to-Peer**, no always on server, arbitrary end systems directly communicate. Peers request service from other peers, provide service in return to other peers

Self-scalability, new peers bring new service capacity, as well as new service demands, peers are intermittently connected and change IP addresses, complex management

**Processes Communicating**

Process: program running within a host.

Sockets, analogous to a door, sending process shoves message out door. Sending process relies on transport infrastructure…

Protocol for application layer is the rule for the application of how it sends its message. Sort of like a title like an invoice has address etc. but says invoice on the top, how you respond to an invoice would be different than how you would treat a transcript you request.

**Notes 10/19/17**

**Application protocol continued:**

Based on TCP/UDP those protocols provide 2 different services, UDP faster but unreliable. TCP more complex but reliable. TCP is used more often since it is more reliable. TCP and UDP is not encrypted passwords are sent as cleartext, SSL provides encrypted TCP connection, data Integrity, and end-point authentication. SSL is at app layer, apps use SSL libraries, that “talk” to TCP.

SSL socket API, cleartext passwords sent into socket traverse internet encrypted.

HTTP is responsible for communication between browser and server.

HTTP(Hypertext transfer protocol): web’s application layer protocol, client/server model

Uses TCP, client initiates TCP connection(creates socket) to server, port 80. Server accepts TCP connection fro client. HTTP messages exchanged between browser and web server.

HTTP is stateless, server maintains no information about past client requests.

HTTP can be non-persistent or persistent.

Persistent remains open until all data is sent. Non-persistent closes after each object is sent.

***COOKIES:***

Many websites use cookies. They create a cookie id when you visit a website. It gets stored in web browser. From the server it uses cookie id as a unique identifying number, it will store all actions a user does on that website with that cookie id. Next time you visit the server you send cookie id http request msg, that server then returns the data that it stored so that the website will be the same state as how you left as long as you still have the cookie stored.

Web Cache’s goal is to satisfy client request without involving origin server.

Conditional Get’s goal: don’t send object if cache has up-to-date cached version

Email is sent from server to server, not from machine to machine.

**Domain Name System(DNS):**

Converts the IP address into a URL address such as google.com to make it easier for users to find and remember the website. It is far easier than just using the IP address as those numbers are difficult to remember. DNS converts the URL address string into an IP address.

DNS is a distributed, hierarchical database.

Notes 10/24/17

[www.southernct.edu](http://www.southernct.edu) is a canonical name

xxx.server.southernct.edu is the actual name

Top level domains such as com org and edu have servers that then have servers for individual websites like yahoo.com

On a first time visit, browser goes to root DNS then goes to the .com or .net or .org server overhead that has a list of all .com .net or .org DNS servers, then it goes to that particular server.

2 kinds of request, iterated and recursive.

Once a name server learns mapping, it caches that mapping.

Cache entries timeout after some time, since IP Address and Host Name mapping may change.

Client server is core of the internet, need those static always on servers to provide the essential service of mapping of different users. This mapping allows a way to find where files are, where users are, the best and fastest way to find something etc.

**Socket Programming:**

Goal: Learn how to build client/server applications that communicate using sockets

Socket: door between application process and end to end something…

SOCK\_DGRAM is for UDP

AF\_INET is IPv4

Notes 10/26/17

**Socket Programming using TCP**

TCP we first need to establish connection between client and server. Need accept function to accept connection from client to server. As long as connection is alive, you can always send a message from client to server and vice versa.

Python TCPCLient

From socket import \*

serverName = ‘servername’

serverPort = 12000

clientSocket = socket(AF\_INET, SOCK\_STREAM)

clientSocket.connect((serverName, serverPort))

sentence = input(‘Input lowercase sentence’)

clientSocket.send(sentence.encode())

continued on slide 10 week 8

Python TCPServer is on slide 11 week 8

serverSocket.listen(1) is maximum amount of connections accepted at a time.

Making a 1-1 chat class - Class Talk:

Server Name = “ “

Server Port = 12000

Client Port = 13000

Define server()

Define client()

Notes 10/31/17

Difference between UDP and TCP is TCP must accept connection first. And TCP must close connection after each use. Need a class, and a plan for developing a socket. Need an attribute and functions. Need a while loop for connection, each time you send message open a new connection then close it after the message has been sent. Non-persistent TCP.

Each person has a server and client side for a 1-1 messaging service. Client sends messages to server.

Class Talk:

ClientIP

ClientPort

ServerPort

Def send() – need to define input and output of function(client)

Loop All: Need read input for user

Create a socket

Connect Server

Send Message

Close Connection

Def receive() – need to define input and output of function(server)

Create a socket

Bind

Listen

Loop All: Accept Connections

Print(or whatever you want to do with messages)

Close Connection

Quiz next Tuesday on everything covered after quiz 1 upto Network Layer

Notes 11/2/2017

Computer Security:

Confidentiality, Integrity and Availability are the three key objects

Confidentiality, means the data you have should not be released to anyone who is not authorized. Basically privacy

Integrity, this means the data should not be modified, deleted or replaced. Data should be kept as original, should never be modified.

Availability, the servers should be available all the time. And service should not be denied to authorized users.

Two others: Accountability, and Authenticity

Authenticity, you should convince the other party of who you are.

Accountability, keep track of all activities of various users. That way you can find out if and who made a mistake or error. Otherwise no one would no who messed up the system.

Breach of Security Levels of Impact:

High, catastrophic impact, on organizations, assets or individuals

Moderate, may have severe impact on organizational operations, assets or individuals

Low, small impact almost no impact to organization, easy to recover very fast on organizational operations, assets, or individuals.

Computer Security Challenges (Slide 7 Week 10)

1. Security is not simple
2. Potential Attacks on the security features need to be considered
3. Procedures used to provide particular services are often counter-intuitive
4. It is necessary to decide where to use the various security mechanisms
5. Security mechanisms typically involve more than a particular algorithm or protocol
6. Security is essentially a battle of wits between a perpetrator and the designer
7. Little benefit from security investment is perceived until a security failure occurs
8. Requires constant monitoring
9. Is too often an afterthought
10. Strong security is often viewed as an impediment to efficient user-friendly operation

OSI Security Architecture:

Security Attack

Security Mechanism

Security Service

Threats and Attacks:

Threat is something dangerous to your system but not happening

Attack is something dangerous actually happening now to your system

Security systems usually consider them the same.

Security Attacks:

Passive, the attack is just to get information on something, but not modify. Hard to detect since it just gathers information

Release of message contents, message sent through internet is captured by 3rd party

Traffic Analysis, they keep track of your network traffic for a long time, package size, package content, when they have a large amount of data they can perform an analysis and decrypt your data

Active

Masquerade, one entity pretends to be a different entity

Replay, involves passive capture(attack) of data unit and its subsequent retransmission to produce an unauthorized effect

Modification of Messages, some portion of legitimate message is altered, or messages are delayed or reordered to produce and unauthorized effect

Denial of Service

Security Services:

Has various definitions.

Contains 14 different items.

According to X.800: (Slide 14 and 15 Week 10)

Authentication

-Peer Entity Authentication

-Data-origin Authentication

Authentication has techniques to let other party know its really the right user. But if user if compromised or device stolen then the virus or whatever can send a message with the correct digital signature

Nonrepudiation is similar but different. More of a legal term, not easy to achieve technically, since if user is compromised Authentication will not work correctly.

Availability Service:

Protects a system to ensure its availability

This service addresses the security concerns raised by denial-of-services attacks

It depends on proper management and control of system resources and thus depends on access control service and other security services.

To design a system of security features you want some level of security:

Economy of Mechanism, trying to make things as simple as possible when designing the system. More complex systems are less user friendly and more vulnerable

Fail-safe defaults, get permission before execution

Complete Mediation, means that every access must be checked against an access control mechanism, sometimes systems use a cache to remember users, but that is not reliable if the system changes/updates as it is a vulnerability.

Open Design, like Linux, since open source more people can look at and improve the system, another example is public and private key schema. Everyone knows how to make public and private keys, the difficulty is how do you make the keys secret and private. Since if you lose a key you will have many problems.

Separation of Privilege, in addition to password and username you need a separate device attached to log in, basically not keeping all privilege in one area

Least of Privilege, privilege by roles, example users have basic privileges, admins have all etc.

Least Common Mechanism, design should minimize the functions shared by different users, providing mutual security.

Psychological Acceptability, the human factor, security should be transparent and cause minimal obstruction. Most vulnerabilities are caused by social engineering

Isolation, applies to three contexts

Public access systems should be isolated from critical resources to prevent disclosure or tampering

Processes and files of individual users should be isolated from one another except where it is explicitly desired

Security mechanisms should be isolated in the sense of preventing access to those mechanisms

Encapsulation, specific case for isolation, protection is provided by encapsulating a collection of procedures and data objects…

Modularity, another type of isolation, in different modules.

Layering, multiple overlapping layers of protection, like username, password, security question, authenticator

Least Astonishment, want to make sure messages are secured, it should be transparent so users understand if the information such as a password is secure or not.

Attack Surfaces: (Slide 37 Week 10)

Attack surface consists of the reachable and exploitable vulnerabilities in a system

Network Attack surface, anything during transmissions

Software Attack surface, software is compromised

Human attack surface, social engineering

Attack Tree:

A branching, hierarchical tree of possible attack paths.

Introduction to Cryptography

Notes 11/7/17

Quiz 3

#3. Difference between switch and router. A switch is a link layer device, a router is a network layer device, so they work on different protocols. Router provides logic layer.

#4.

1111010101110110

1000111101001011

11000010011000001

1000010011000010

Take complement. 0111101100111101

#5. Address Resolution Protocol, links MAC address to IP addresses

B | A Divisibility

3 | 24

Proofs

Formal Definition of Division

A = qn + r 0 <= r < n; q = |\_ a/n \_|

/ versus %

Euclidean Algorithm

Two integers are relatively prime if their only common positive integer factor is 1.

Greatest Common Divisor(GCD)

GCD of a and b is largest integer that divides both a and b, use the notation gcd(a,b) to mean the greatest common divisor of a and b

Gcd(a,b) = max[k, such that k|a and k|b]

Notes 11/16/17

12:45-2:45 Thursday on finals week December 14

Meet with Professor about group progress. Test after thanksgiving on cryptography

Week 11 and Week 12

Block Cipher

FunFacts[As time goes on encryption weakens, slightly as processing power increases. Quantum computing will most likely make encryption outdated. Quantum computing may also save space, since it can hold many states in one quantum as opposed to bits having one state.]

Stream Cipher – string of characters use a substitution algorithm, think Caesar cipher. For the project you can use any type of encryption. Although advanced encryption are easier as they have a lot of libraries.

Block Cipher- main stream of symmetric encryption. Encrypt bits by bits or bytes by bytes, for block you treat end bits as a whole, then you encrypt the whole block. Usually 4, 16, 64, 128 for size of blocks. Trying to find a mapping.

Key size being to large is impractical. Instead have a method to approximate the ideal block size of the key.

Feistel Cipher, base of modern symmetric block cipher. Uses a combination of substitution and permutation to emulate all the statistical features of block cipher.

Diffusion, statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits. Makes relationship between original and cipher text as complex as possible so you cant figure out relationship

Confusion, makes relationship between key and cipher text as complex as possible so you cant figure out relationship

Feistel Cipher generates a cipher key during encryption, breaks first 32 bits as left, and next 32 bits as right. 16 total rounds

Fundamental parts of Feistel Cipher: Slide 10 Week 11

Block Size

Key Size

Number of Rounds

Subkey Generation algorithms

Round Function F

Fast Software encrypt/decrypt

Ease of Analysis

Advanced Encryption Standard (AES)

Has 10/12/14 rounds

4 Different steps: Slide 23 Week 11

Substitute Bytes

Shift Rows

Mix Columns

Add Round Key

Notes 11/21/17

Quiz 3 covers Week 10, 12, 13

Asymmetric Encryption:

Principles of Public-Key cryptosystems:

Plaintext

Encryption algorithm

Public Key

Private Key

Cipher Text

Decryption

Public-Key Cryptosystems

Encryption/decryption

Digital signature

Key exchange

Public-Key Requirements

The algorithms must fulfill certain criteria: Week 13 Slide 13

Write down the criteria for these, most likely will be on the next quiz Week 13 Slide 15

Week 13 Slide 19

Smaller key is faster to compute but easier to break

You have to find a tradeoff between a small enough number to be secure, and a large enough number to Key Distribution: Slide 3 Week 13

Symmetric Key Distribution

Notes 11/28/17

Final exam is online, must download slides and ebook, no online/google at all

Week 14 Authentication

Nonce: number (R) used only once-in-a-lifetime

Ap4.0: to prove Alice “live”, Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key.

Ap4.0 requires a shared symmetric key

AP5.0 use nonce, public key cryptography

Tough to detect since both parties receive all the information but a third party can also receive the information which would be a security flaw.

Hash Function compresses file size down, they are used to ensure data integrity.

A disadvantage of public key/private key is large number size

SSL: Secure Sockets Layer

-widely deployed security protocol

SSL inner workings are not on final exam. You do need to know what it does to security etc.

VPNs