What is the internet

* The internet was originally created to be a distributed network capable of surviving an attack
* No one controls the internet
* Completely distributed network where no one has control of how or where the packets flow
* Access is granted and facilitated by ISPs

Wires Cables Wifi

* Data is transferred similarly to mail.
* Instead of letters, the messages being sent are comprised of 0's and 1's called bits
* Bits are assembled into groups of 8 called bytes
* Bits can be thought of atoms that make up data
* Today we send bits through 3 main mediums (electricity, light, radio)
* Bandwidth - transmission capacity, measured by bitrate
* Bitrate - number of bits per second a system can transmit
* Latency - time it takes for a bit to travel from sender to receiver
* Ethernet (copper wires) allow for cheap data transfer of electrical signals. They suffer data loss and interference very quickly over long distances
* Fiber (optical wires) allow for fast data transfer of light signals. They are also extremely efficient and suffer little too no loss even at large distances. Expensive cables and very hard to work with.
* Radio signals (wireless) allow for transfer of data without physical connections. Bits are translated into different wave lengths based on different frequencies and then translated back into data at the receiving end. Signal loss is great at distances (distance varies depending on frequency i.e. AM vs FM)
* Wi-Fi takes local radio waves and converts them into copper or fiber messages to be sent over the physical network
* Future may bring about new ways to share data but elementary bits concept will likely remain.

IP Addresses and DNS

* Initially there was no standard in packet sending.
* Internetworking Protocol (IP) was developed by Vint Cerf and Bob Kahn
* Internet is a network of networks
* Local networks (i.e. devices like laptops and cellphones connected to home wifi router) are then connected to a greater network through an ISP (internet service provider). The ISP then connects you too other ISPs and networks that are all interconnected
* Internet is a design philosophy and architecture expressed in a set of protocols
* Protocol - well known set of rules and standards that all parties agree to use to communicate between machines
* This has allowed the expansion of the internet and internet capable devices due to uniform standards (i.e. which protocols to use and work with)
* All devices on the internet have a unique address (just a number) within a given network
* These unique IP addresses work similar to mailing addresses
* Visiting a website can be broken down / thought of as your computer sending mail with the IP address of the website as the recipient address and a return address of your computer. This allows the website to return information to you in the same manner.
* IP addresses can be broken down into several parts
* Traditional IP addresses are 32 bits long (8 bits for each of the 4 parts)
* The IP addresses used to be broken down into country/region/subnetwork/device
* This is IPv4 (designed in 1973 and adopted in 1980s
* Allowed up to 4 billion unique addresses (devices) to be connected to the internet
* The world is currently in transition to IPv6
* IPv6 uses 128 bits per address (8 segments of 4 hexadecimal characters)
* Most people never know or see actual IP addresses due to DNS
* DNS - domain name server is a lookup that corelates names to addresses
* DNS servers are broken up in a manner that dedicates certain servers to handle certain website types (i.e. some handle .com while others handle .org)
* DNS was originally designed to be an open and public communication protocol
* Due to its openness, it is susceptible to cyber attacks like DNS spoofing
* This allows malicious users to reroute unknowing users to fake or incorrect websites
* Both DNS and IP addresses were designed with scalability in mind

Packets, Routing, and Reliability

* Data transfers on the internet are not point to point but very indirect
* Paths can change extremely often, even during a transmission
* Packets are data traveling along the internet and work more like cars than trains.
* Packets are allowed to take any available road (whether it is the most efficient route or not)
* Packets can contain almost any type of data and depending on size, messages may be broken up into several packets
* Groups of packets can take diverging paths and arrive at the destination at different times and potentially out of order
* Packets simply carry the data as well as headers containing to and from addresses and are moved through the networks via Routers
* Routers act like traffic managers to keep packets moving smoothly through the network
* Routers attempt to push packets through the "cheapest" available path at any given moment
* Having multiple routes allows the network to be fault tolerant (i.e. multiple roads can be closed or blocked but packages can still get to their end destination)
* TCP (transmission control protocol) - manages the sending and receiving of all your data packets (i.e. guaranteed mail service where TCP validates all packets have been received) so that when all packets are received they can be reassembled
* TCP and Routing were built with scalability in mind. More routers = more redundancy

HTTP and HTML

* To access the internet, you use a web browser to enter the URL (uniform resource locator) of a webpage
* Your computer then reaches out to a DNS which seems HTTP responses back to your computer
* HTTP - hypertext transfer protocol, the language used to communicate between web browsers and servers
* Relatively simple messages mainly made up of get requests
* Get requests are simple lookup requests (i.e. get document-name or get /login)
* HTML - hypertext markup language, the language used to tell a web browser how a page should look
* HTML is made up of tags for fonts, links, images, formatting, alignment, etc.
* Images and videos are not included in HTML but see separate files that are linked to via separate URLs
* These requests are handled via separate HTTP requests from the main page and are displayed as they come in
* Obviously the more image, video, other HTTP requests, the slower a page loads
* When sending information to a server, your computer sends Post requests to servers (i.e. post requests to websites with login information)
* Cookies - temporary files that allow websites to save data and remember things like who you are
* HTTP communications are handled via plain text requests and are susceptible to hackers and other security vulnerabilities
* This led to creation of SSL (secure socket layer) and TSL (transport layer security) incorporated into HTTPS
* This is done via digital certificates that provided by verified websites
* If the certificates being sent by websites have not been verified, you web browser will warn you

Encryption Public Keys

* Encryption (scrambling or changing a message to hide it) allows us to safely transfer private data over the open and unsecured internet
* Decryption is the process of unscrambling am encrypted message to make it readable
* Caesar's Cypher was one of the first encryption methods
* Based on Caesar's idea of "encrypting" messages so that intercepted messages were unreadable to his enemies, letters in the messages were shifted a certain amount of letters up or down in the alphabet (i.e. all letters were shifted up or down 3 letters)
* Keys are the amount of letters that a sender and receiver have agreed upon so that the messages can be unlocked
* HELLO with a key of 5 would be MJQQT
* This cypher is extremely simple and easy to crack (brute force would only take at most 26 different shift combinations)
* A 10 digit encryption key on the other hand would create 10 billion possible solutions
* While this would take a human centuries it would still only take a computer seconds
* Today's encryption keys are 256 bits
* Symmetric encryption is when the same key is used to encrypt and decrypt messages
* Asymmetric encryption is what is used by communication on the internet
* There is a public key for encrypting and a private key for decrypting
* Public key is shared so that anyone can encrypt messages (normally sent by websites to clients)
* This way messages can only be decrypted once received back to website servers via their private keys
* Public keys can open delivery slots on mailboxes, private keys can open the mailbox
* This pubic / private key encryption methods is the basis for SSL and TLS encryption protocols
* Web browsers indicate this with the lock icon and https

Cybersecurity Crime

* Cyber crimes are on the rise
* From stolen credit cards and identities to nuclear power plants and drones, almost nothing is off limits to malicious actors
* Vulnerabilities in both hardware and software are exploited
* Sometimes vulnerabilities are simply decisions made by people using software that developers did not intend or account for
* Cyber crimes are committed by malicious terrorists and state actors as well as bored teenagers looking for bragging rights
* Most countries now have a dedicated cyber security "army"
* Estimated that the next world war will be one of cyber warfare (i.e. disruptions in water, electrical, or transportation systems of countries)
* Computer Virus is similar to real world virus
* Normally installed unintentionally
* Hand user and their computer
* Possible to spread to other computers
* Vírus creators tend to trick people into installing software via false pretenses (i.e. a fake "security" update)
* Vírus can also enter a computer system via a system or software vulnerability (bypassing need to be installed by user)
* Depending on the virus it can steal or delete data, control programs, or grant remote operation or access
* Vírus can also be used to infect and control computers in the form of a "BotNet"
* BotNets can then be used to perform DDoS (distributed denial of service) attacks
* This is when websites are overwhelmed with too many requests at once from various sources
* Phishing - trick users into sharing personal or sensitive data, usually in the form of fake emails
* These emails normally link to fake websites where users give the fake website their real user name and password
* 90% of system hacks are not due to software or system vulnerabilities but instead human mistakes
* Use strong passwords
* Verify authentic web addresses
* Stay up to date with security patches
* Don't install software from unknown sources