3.1 Networks and 3.2 Security

Notebook:	How Computers Work [CM1030]		
Created:	2019-10-09 10:09 AM	**Updated:**	2019-10-19 2:11 PM
Author:	SUKHJIT MANN		
Tags:	2FA, Encryption, Internet, ISP, Network, Security, Virus		

Cornell Notes	**Topic:** 3.1 Networks, 3.2 Security	Course: BSc Computer Science
		Class: How Computer Work [CM1030}
		Date: October 19, 2019

Essential Question:

- How do computers communicate with each other and what security measures can be put in place to ensure the safety of computers, their contents and their messages?

Questions/Cues:

- What is a network?
- What is bandwidth?
- What are protocols?
- What is the internet?
- What is a Router?
- What is a ISP and IP Address?
- What is a Packet?
- What is an URL?
- What is Domain Name and the Domain Name Service?
- What is Virus?
- What is Spyware?
- What is a Trojan Horse?
- What is Phishing?
- What is Encryption
- What is an Encryption Key or Key?
- What is Public Key Encryption?
- What is a Certificate?

Notes

- Network = # of comps connected by links, like a fishing net
  - Traditionally comps connected using wires
  - Cooper cables replaced by fiber-optic or wireless
- Fibre-optic = signals sent via light
- Wireless = comms via electromagnetic waves which require no physically connected comp
- Bandwidth = amount of data that can be sent over a network within given time
  - "How fast" network is

- Reliability = msg sent over network will get to destination
    - Wired networks super reliable b/c wire from one comp to another
    - Wireless unreliable b/c of bad signal strength (walls or obstacles), or too many people on network
- Bandwidth and Reliability effect Network Performance
- Protocols = lang used for network comms
    - Not like human langs, very strict rules
    - Protocol defines rules on how to communicate
- Wifi and Cell networks same basic tech, but cell network longer range and generally lower bandwidth than Wifi, diff protocols for comms
- Internet = network of networks, connects together diff networks, allows comps to communicate with other comps across diff networks
- Router = connects together 2 networks, forwarding msgs from 1 network to other, also translating between network protocols
- When we use internet, we connect local network, local nets don't directly comm with each other
- ISP (Internet Service Provider) = big networks, span whole countries, evolution of old wired telephone nets
    - Nationalized ISPs are connected to International ISPs, called the Internet Backbone
- Packet = like virtual envelope with internet address and other info
- IP Msg wrapped in wifi protocol and sent to home router → ISP protocol envelope
- Emails use Send-mail protocol, web pages used HTTP Protocol
- Every Comp on Internet has IP Address, know IP address allows routers to reach comp
- URL(Uniform Resource Locator) = human-friendly version of IP Address
    - middle part of URL = domain name, name of server where site is stored
    - Domain name is converted to IP Address using Internet Service called Domain Name Service or DNS
- Virus = software that copies itself from one comp to another without user knowledge, aimed at damaging comp
    - slows down comp, interferes with OS, or stealing data from comp
- Spyware = records what you do on comp and sends to third party
    - recording what you type on keyboard, getting password
- Trojan Horse = appears to be legit software, but performs harmful actions in secret
- Hacking = getting access to system that you had no previous access to; to steal data
    - Hackers normally go after web servers or internet servers that have lots of data, rather than indiv comp
- Phishing = fooled into giving password or bank details, through a plausible-looking site or email that looks like from bank or similar; controlled by criminals
- Encryption = sending msgs in codes, so can only be read by person who is supposed to receive them
    - Code in special language cannot be read unless you know code
- Encryption Algorithm = series of math operations converts text into another form
    - designed so msg cannot be deciphered, even if all details of encrypt algo are known as long as key unknown
- Encryption Key or Key = a # that controls how encrypt algo works
- Public Key Encryption = diff keys used to encrypt msg and to decrypt it
    - Encrypt key is public, so anyone can used to create encrypt msg; only people with decrypt key can read msg
- Certificate = to demonstrate validity of public key; keys and certs issued by # of trusted security companies
    - Web browser can check trustworthiness of certs
- Antivirus Software = includes info on all known virus and searches comp for them
- Firewall = stops suspect-looking msgs from coming in or out of comp
    - prevents direct hacking of comp
- Access Control = certain people can have access to comp or server
    - Done by making people log-in with username and password

    - Diff people have access to diff parts on comp or server to do what they need, but can't damage it accidentally or deliberately
    - Rely on passwords (always encrypted, some easy to guess)
- 2FA (Two factor authentication) = includes password, but require to enter passcode that site sends to mobile phone

Summary

In this week, we learned how computer communicate with each other, what the internet is and the different protocols required to do communications over networks. Alongside this, we learned about potential security threats to our information when using the internet and ways to effectively ensure the safe use of our time on the internet when communicating and storing sensitive information.