14.1 Network Security-Reading

Notebook:	How Computers Work [CM1030]		
Created:	2019-10-09 10:09 AM	**Updated:**	2020-01-13 6:25 PM
Author:	SUKHJIT MANN		

Cornell Notes	**Topic:** 14.1 Network Security-Reading	Course: BSc Computer Science Class: How Computer Work [CM1030]-Reading Date: January 13, 2020

Essential Question:

What are the various ways in which the security of a network can be compromised?

Questions/Cues:

- What is a virus?
- What is a worm?
- What is a Trojan horse?
- What is Spyware?
- What is phishing?
- What is DoS attack?
- What is a firewall?
- What is Spoofing?
- What is a spam filter?
- What is a proxy server?
- What is anti-virus software?
- What is SSL?
- What is public-key encryption?
- Who are the certificate authorities and what are certificates?
- What is authentication?

Notes

- Virus = software that infects comp by inserting itself into progs that already reside in machine. When "host" prog is executed, virus is executed. When executed, virus try to copy itself to other progs. Some viruses perform actions like degrading portions of OS, erasing large blocks or otherwise corrupting data & other progs
- Worm = autonomous prog that transfers itself through a network taking up residence in comp & forwarding copies of itself to other comps. Like a virus, worm can copy itself or perform extreme actions. Consequence of worm is an explosion of the worm's replicated copies that degrade performance of legit apps & can lead to overload of entire network or internet
- Trojan horse = enters comp disguised as desirable prog, imported by user. Once in comp, TH performs additional activities harmful with effects; additional activities start immediately. In other cases, TH may lie dormant until triggered by specific event such as a date.

- Spyware = sniffing software that collects info about activities at comp on it resides & reports that info back to designer
- Phishing = technique of obtaining info explicitly by simply asking for it. Process involves casting numerous "lines" in hopes someone will "take the bait"
- DoS (Denial of Service) attack = process of overloading a comp with msgs. To accomplish this, attacker usually plants software on numerous unsuspecting comps that will generate msgs when a signal is given(called botnet). When signal given, botnet swamp target with msgs
- Firewall = filtering traffic passing through a point in network.
- Spoofing = Masquerading as a party other than one's self
- Spam filters = firewalls designed to block unwanted email
- Proxy server = software unit that acts as an intermediary between client & server with goal of shielding client from adverse actions of server. PS filters all msgs from server to client.
- Anti-virus software = used to detect & remove presence of known viruses & other infections
- SSL(Secure Sockets Layer) = provide secure comm links between web clients & servers
- Public-key encryption = involves techniques by which encryption systems are designed so that having knowledge about how msgs are encrypted does not allow one to decrypt msgs. PKE system involves use of values called keys, one called public key (used to encrypt msgs), the other key known as private key (used to decrypt msgs)
- Certificate authorities = whose task is to maintain accurate lists of parties & their public keys. These authorities then acting as severs, provide reliable public-key info to their clients in packages known as certificates.
- Certificate = package containing a party's name and that party's public key
- Authentication = making sure the author of msg is in fact, the party it claims to be.
- Digital Signature = a bit pattern produced by the holder a private key that encrypts their msgs. A pattern that only they can produce. A digital signature can be as simple as the encrypted version of the msg itself.

Summary

In this week, we learned the dangers to network security & remedies to a few such attacks.