# CS370 Notes

week 9

## Malware

- Malicious software that violates a security policy

Virus: Attaches to program, hops to other programs | (and worms) use UDP packets, no Ack. Can spread by drive-by (websites)

Trojan: Contains unexpected functionality

Logic Bomb: triggers on logic event

Time Bomb: triggers at a given time

Trapdoor: allows unauthorized access to functionality

Viruses:
Dormant - waiting
Propagate - replicate to other locations
Triggering - triggered
Execution - executes payload
- can attach to programs (start or end, or within), (more below)

Worm: propagates through network, Dormant, spread, trigger, execute payload

Rabbit: replicates to exhaust resources

Netbot: trapdoor orchestrated through control channel

Root Kit: hooks OS cals to hide data
↳ breaks syscall table ptrs, stays hidden

How does malware get onto computers?
→ everything from USB's to SQL vulns

IPV6: It is much harder to find good hosts

Virus Scanner Generations
- 1] signatures
2] Heuristics and integrity checks
3] behavior based
4] Multiple.

Zero Day
- no patch when vuln is discovered/released

Blue Pill Rootkit
- installs a hypervisor layer

Worms scan in patterns - this can be recognized and the worm can be found.

Macros Viruses
- Mobile code, interpreted not compiled
- interpreted by file running the program
- appear to be ~~seen~~ data, not code
- check hashes; don't trust anyone
- Scan for viruses (though <50% effec.)
- used to be able to scan for signatures, not anymore
↳ polymorphic: many different but same-functioning copies of virus
↳ stealth: tries to hide signature
↳ Encrypted: most is encrypted
↳ Metamorphic: complete rewrite on each infection