IS Threats; class 4

06/02

# Origin of security incidents:

Internal accidents > external accidents

# History of Hacking

1971: “CREEPER”, on ARPANET was not malicious

1974: game “Animal”, if the user didn’t have an up to date version of the game, it installed the latest version of it

1982: first virus for Apple II, distributed by floppy disks

Xerox research center, distributed itself on all the network

1986: First track of viruses on PCs, on floppy disk. Pretends to be a defective element of the disk

1988: Great worm infects 10% of the internet

1996: First virus for Linux, ‘Staog” laboratory virus only

1998: Macro and Java viruses, can run on all the systems

2006: Cyber extortion: ransom against destruction of information, restitution in exchange of payment

2007: Cyberattack in Estonia

May 2017: WannaCry, infected 300 000 computers

June 2017: NotPetya, wiper masquerading as ransomware

January 2018: Meltdown and Spectre Attack: affecting the microprocessors. Breaks memory isolation between users, programs, ...

# Kind of Malwares

**Physical keyloggers**: plug between computer / keyboard or mouse. It stoles what you’re writing.

**Software keyloggers**: video observations, stores the data types on the keyword, intercepts browsing…

Objective of the keylogger : get the loggins & data stored on the computer

**Virus** :

* you have to launch it manually
* It infects other programs

**Worm** :

* No need human activation
* Malicious purpose
* Goal is to reproduce itself
* Has a signature

**Trojan**:

* Appear legitimate but contains malicious functionality
* Used a lot in cracked free software

**Adware**:

* Manage displaying advertising
* Usually not aggressive
* Can change the DNS server to redirect toward advertising

**Downloader**:

* Waits for internet to download additional programs
* May be distributed as a file attachment in spam emails

**Rootkit**:

* Collection of software to enable access to a computer while masking its existence

Vulnerabilities are increasing ! The reasons are:

* No security in projects
* Complexity of IS
* Marketing requirements
* Too fast evolving technologies

# 

# Kind of attacks

* Hacking
  + Exploits
    - Principle: exploit a vulnerability
    - Aims: system takeover, cause error
    - Creation: Script, Payload, Distribution
    - Vulnerabilities: Buffer, Heap, Integer, Stack Overflow & Code injection
* DDOS
  + Principle: mute a server by overflowing it
  + Need many computers to submerge a server
    - Best equipment to create a botnet : phone. It is always connected.
  + A master with C&C and many distant hosts daemons
  + Average 20 000 hosts
* Cryptography
  + Side channel attacks
    - Review power consumption
    - Radio emissions
    - Measuring relative operation time
  + Man in the middle
    - Observe and intercept message
    - Not being noticed
    - Capture public keys during exchanges
  + Replay attacks
    - Captures and resubmits it to fool receiver to be authenticated
    - Use timestamps as a countermeasure
  + Brute force
    - Test all possibility, at some point one will work
* Technical attacks
  + Buffer overflow
    - Overwrite return address stored in buffer, can write a specific address for it to return to, it is your shell code. Write nop before shell code for higher chance
  + DNS spoofing
    - Redirects to malicious website
    - Send the answer back to DNS request before the real one does. Has to guess id, so can flood with ids to find one and be accepted.
  + DNS cache poisoning
    - Modify the cache for the correspondence between a name and an ip address
* Web
  + URL manipulation
    - Access to admin interface or non public information
  + XSS
    - Get cookies
    - Execute javascript
  + CSRF
    - Run script from link for authenticated user
  + SQL Injection
    - SQL statement are inserted into a field
* Fraud
  + Social Engineering
    - Obtain information or to perform some action
  + Phishing
    - Obtain sensitive information
    - Commit identity theft

# Scenario of Advanced Persistent Threat

1. Hack a user’s computer from the internet with trapped website or malicious email
2. Running a Trojan and communicate with a server on the internet
3. Internal network mapping
4. Attack and take control of servers (typically the server with credentials like Active Directory)
5. Exfiltration of passwords
6. Taking control of other computers in the network
7. Content exfiltration
8. Erasing traces of exfiltration