CS607 - Security & Viruses

Methods of Authentification

In order to restrict unauthorised access to a system, authorised users must be able to prove their identity. This is done by using one or more of the following:

1 Something you know

e.g. password

2 Something you have

e.g. a magnetic strip

3 Something unique to you

e.g. a finger print

Using these methods in combination with each other can increase the security of your system

Nr of methods	Description	Example
1	One-factor security system	*Login*: Password (1)
2	Two-factor security system	*ATM:* Magnetic Srip (2) PIN (1)
3	Three-factor security system	*Passport:* Passport (2) Photo (3) Signature (1)

Passwords

The most common way of compromising password protected systems is to discover the password.

There are several ways that this can be done

Dictionary Attack

Programs can be used to try to login to a system using a variety of passwords. Dictionary Attacks involve trying every word in the dictionary in order to guess the password. Dictionary files can include technical terms, actors/singers names and so on. Dictonary attacks can also check for several words used together (e.g. "anger*bovine"),* words spelled backwards, and words with numbers appended or prepended (e.g. "bovine23").

Brute Force Attack

Tries every combination of every letter in the alphabet (as well as other characters). Brute force attcks can be very time consuming. The longer the password the longer it will take to *crack.*

e.g.
A, B, C, D ....., Z
AA, AB, ..., AZ, BA, BB, ..., BZ, CA, CB..... ZZ
AAA, AAB, ...

Password Grabbers

Password Grabbers intercept passwords after they have been typed in. This can be done in the following ways:

- Passwords can be detected as they travel along networks

- A program can be written that records every key pressed on a PC. if someone logs in to a system their password will be recorded.

- Some programs can emulate a login prompt. The user, thinking they are at the proper login prompt type in their password which can be sent on to another party.

Default Passwords

Many systems come with default passwords built in. Similarly, new accounts frequently have default passwords (e.g. student IDs), some even have the account name used as the password. These are easily exploited if they aren't changed immediately.

Observation

People can be seen typing in passwords.

Obvious Passwords

Nicknames, names of friends, spouses, etc. are easily guessable. Especially by people who know you.

Indiscretion

Writing down passwords, telling them to friends, etc.

"**Social Engineering**"

Acquiring passwords by false pretences (usually on the phone). Social Engineers typically ring up people claiming to be a system administrator. They might pretend that there is a fault at their end and that they need your password to fix it (System administrators should *never* need your password).

Maximising Password Protection

In order to maximise password protection, you should use a password which is as difficult as possible to crack. Below are listed some tips, along with the hazard they are meant to counteract.

Do Not Use

Your Name Spouse's Name Friend's Name Nick Names etc.	*Obvious*
Name of operating system Names of fictional characters Names of favourite songs " singers " Actors " films etc	*Obvious, Dictionary*
Any Date (e.g. birthday)	*Obvious, Dictionary, Brute Force*
Repeated Characters	*Obvious, Observation*
Very short password	*Brute Force*
Any of the above backwards or prepended by a digit	*Dictionary, Obvious*
The same password on multiple machines	*Indiscretion*

Don't

Write your password down Give it to anyone	*Indiscretion*
Type in your password when people are watching	*Observation, Indiscrete*
Allow unlimited attempts at guessing passwords	*Dictionary, Brute Force*

Do

Use over 6 characters	*Brute Force*
Use uppercase and lowercase e.g. "EtyPTl"	*Dictionary, Brute Force*
Make it easy to remember e.g. "AsTiTcHiNtImE" "sTtChNtM" (no vowels)	*Indiscretion, Observation*
Change your password often	*all*
Pick a password that can be typed quickly	*Observation*
Pick a password that contains digits and punctuation e.g. " AsT1Tc#1Nt1m@"	*Dictionary, Brute Force*

Viruses

The first virus was written by Fred Cohen in 1983 to demonstrate security holes.

> "A virus is a program that can infect other programs by modifying them to include a possibly evolved version of itself" - Fred Cohen

- They are usually unstoppable, even by the authors themselves.

• They can only cause logical (not physical) damage.

Viruses have 2 functions

1) Cloning themselves.

2) Delivering a payload (performing an action when *triggered*).

Cloning Themselves

Viruses, when run, add their code to existing files so that their new code will be run along with the code that they infected.

File Infectors: Viruses which attack executable files.

Boot Infectors: Viruses which infect the boot sector of disk.

Multipartite Viruses: Can infect both files and boot sectors.

Delivering The Payload

Once a virus is *triggered* it performs an *action*.

Triggers

A virus may deliver its payload as soon as it is first activated, or wait until a trigger is activated (usually a particular date or the number of times the file has been executed).

Actions

When triggered, viruses can:

Delete files
Stop computers starting up
Swap characters on screen
Clone themselves until a disk fills
Display message
Crash machines

Detecting Viruses

To counteract viruses, special programs - called virus *scanners* or *detectors* - are used to check if your disk has been infected by a virus. These programs use a vairiety of tecnhiques to detect the viruses.

File Lengths

A virus will increase the length/size of the file that infects . A virus scanner can record the length of every file on a disk every time it is run. It also checks the current file sizes against the file sizes it recorded the last time it was run. Any file sizes which are unaccountably larger are considered to have been infected. Files which have been modified by the user between both scans should be discounted.

Time Stamps

Each file stored on a disk has a timestamp stored with it. This is a record of the time and date that the file was last modified. Since viruses modify files, the timestamp is also changed. The virus scanner can record timestamps in the same way as file lengths.

Virus Activity

When a virus is cloning itself or performing some action it takes up CPU resources. Programs can be used to monitor CPU activity so that when the virus begins to clone itself it will be detected. The virus may also have other effects on the system. Programs will take longer to load into main memory (since the virus is also being loaded), programs will have slower execution times (since the virus is also executing), less RAM will be available (since the virus takes up extra memory).

Signatures

Each type of virus has a unique signature which identifies it. This is normally a bit pattern or string. If a scanner knows the signature it can easily find the virus by scanning disk for known signature. In order for these scanners to work they must have an up-to-date list of these signatures. Their effectiveness will depend on this. Usually, companies who sell these scanners provide regular updates. Updates are also available over the internet.

File Changes

Viruses alter the contents of files. Techniques are available to detect these changes. These are usually mathematical in nature (considering the file as a binary number or a polynomial).

Types of Virus

In order to avoid detection, viruses have developed countermeasures.

Polymorphic Viruses

These viruses create different copies of themselves when cloning so that they have no detectable signatures.

(avoids detections by signature based scanners)

Sparse Infectors

Infects files only occasionally to reduce the probability of being discovered.

(activity monitors)

Fast Infectors

Infect both executable and open files, e.g. if a virus scanner is used, every file it scans can be infected.

Slow Infectors

If active, they infect only files that are being modified. This means that the contents of the file are changed by the user and the virus at the same time.

(time stamp, file size, checksum etc)

Stealth Viruses

Can hide the modifications it has made to bootsectors or files from virus scanners by monitoring the system functions used by the scanner and forging the results so that the infected file appears normal, e.g. change the timestamp so that it reads the time that the file had last been changed before it was infected.

(file size, timestamp)

Virus Disenfectants

These are programs which try to retore infected files to their original form. This can be risky since they alter files. The best solution to a virus infection is to delete infected files.

Virus Prevention

- Be wary of downloaded software
- Write protect disk/files if possible
- Scan all new software
- Scan all files before making backups

Trojan Horses

These are programs which have functions, typically malicious, other than those it advertises. They are non-replicating.

e.g. "AIDS Information introductory disk version 2.0". This program came with a magazine and evaluated your chances of having AIDS but also deleted files.

A common Trojan Horse writes a fake login procedure which grabs passwords.