Tutorial 2

Aim

To exemplify

- security mechanisms and their effect on usability and functionality
- attack methods

Questions

1. A specific security mechanism protects against a certain type of threat. Most antivirus software has an explicit list of malware fingerprint (binary code pattern) that it can identify and neutralise. What type of malware can be identified in this way, and what type of malware may remain hidden? Discuss.

Types of Threats

Malware unwanted, probably malicious software

It includes: Viruses, worms, Trojan horses, rootkits, spyware, adware etc.

Viruses (Infection)

- The program that can copy itself and infects (attaches itself to) other programs by adding their own code to them to gain control of the infected files when they are opened.
- For virus to spread it needs to be attached to other program, and be executed by user.
- Corrupts / modifies files on target computer.

Worms

- Self-replicating malware / computer program. It uses computer network to send copies of itself to other computers on network (without any user intervention).
- Worms does not need to attach itself to any program to spread itself.
- Consumes network bandwidth, exploits operating system vulnerabilities.
- E.g. Blaster worm
  - The worm spread by exploiting buffer overflow. Contained two messages:
    - I just want to say LOVE YOU SAN!!
    - Billy Gates why do you make this possible? Stop making money and fix your software!!
  - Puts the entry into the registry so that it is launched every time Windows starts:
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update = msblast.exe

Trojan horses

- “It is a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems”
- It can carry out unauthorised action on computers
  - Deleting information on drives, making system hang, stealing confidential information (does not affect other computers or data). Damage may exceed that done by traditional virus attacks.

Spyware

- Software that collects (little bits of) information about a particular user or organization without their knowledge.

- You might never know / guess that you have spyware installed, it is difficult to detect.
- E.g. keyloggers (installed by owner of shared / public computer – to secretly monitor user activity)
- Apart from simply collecting information it can also redirect web request, install other softwares, change computer settings etc...

Adware

- Displays advertisements on user computer in undesirable places, displays pop-ups, and installs toolbars without prior mentioning.
- Used to generate revenue for the creator of adware.

Rootkits (root = administrator user account + kit = software)

- It is a software / hardware device designed to gain administrator-level control over a computer system without being detected.
- It modifies the OS on computer and alters the basic functions to hide its own existence and actions that the hacker undertakes on the infected computer.
- Targets: BIOS, boot loader, kernel, (less commonly libraries, applications)

Trapdoor / Backdoor

- Backdoor in a computer system is a method of bypassing normal authentication, gaining remote access to computer and collecting information while attempting to remain undetected.
- It can take form of installed program or could modify the existing program.

Logic bomb

- It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.
- E.g. delete all computer files when being terminated from the company.

Easter egg

- Non harmful: hidden message in the program.
- E.g. Microsoft Office 97: Word contained hidden pinball game, Excel contained flight simulator. Microsoft Office 2000 Excel: Racing game.

Antivirus Software:

- Signature based detection and removal. (works for existing signatures)
- For Zero-day threats – heuristics can be used / Sandbox is other method.
- ONLY works for the signature that is known to the antivirus program.

What Antivirus can detect:

- ONLY those types of Malware for which the definition exists in the database.
- Malware (Viruses, Worms, Trojan horses, Adware, Spyware and other malware)

What Antivirus cannot detect:

- Malware whose definition is not in the database.
    - New viruses, e.g. because the signature database is not up to date.

2. Security is often said to interfere with usability and in some cases with functionality as well. Explain how this applies to the case when you use your Windows computer account at RMIT.

WHY do we enforce security policies? Because once the malware is within the RMIT network, it is much harder to remove and it will infect more systems, so try to keep it out

Features reducing usability

- Blocked access to specific sites (P2P sites, torrent sites, etc...)
- Blocked protocols / ports
- JavaScript disabled on some browser / OS
- Cannot install Software / Programs
- Cannot modify System Settings (date-time, wallpaper, etc...)
- Password expiration policy
- No previous 5 passwords
- Password complexity
- Relatively slower response to web
- Network Disk may cause accessibility issue

3. A common attack method is social engineering. Imagine a scenario where someone wants to obtain your RMIT username and password in this way.
   - (a) Describe the scenario.
   - (b) Identify the components in this attack, such as vulnerability, exploit, threat agent and threat
   - (c) Devise some methods to thwart such an attack.

Social engineering: manipulating people into performing actions or revealing confidential information without raising suspicion and rather than breaking in or using a technical approach.

- The information can be used to steal data or money, to gain access to systems, etc

(a)

- Phone call
  You just enrolled and ITS gives you a call and asks your username / password (your account is not setup properly and we need these details)
- Shoulder surfing
  You are doing a group assignment and fellow asks for your username / password to work on it later

(b)

- Vulnerability (weakness)
  - Your name / student id on the RMIT website
  - Personal email ID containing student number
  - Lack of education about computer security
  - You being too frank to strangers
  - Lots of information on Facebook, Twitter, Picasa
- Exploit (technique that allows attacker to take advantage of vulnerabilities)
  - Find username from the RMIT Email Search system
  - During the start of the week, try default password
  - Pretend that your account is not working on your personal machine – Ask the victim to try with his details.
  - Recording a session of the victim and re-use it
    - Shoulder surfing (Look over shoulder)
    - Video recording while typing the password. (using mobile camera, etc)
  - Importance of Past activities:
    - Threat is not one off. Usually a numbers of steps are required to make the exploit work. E.g.
      - Keylogger needs to gather the username / password
      - To make exploit work, one must know on what URL that username / password will work.
- Threat agent (Capabilities + Intentions + Past Activities)
  - When a program / malware is running; itself is the threat agent.
- Threat (The potentially harmful event)
  - Theft of assignment
  - Deleting files / assignment
  - Gain more access to personal information

(c)

- Be aware of your surrounding
- Avoid the use of public computer / someone else's computer
- Beware of persistent cookies (Gmail) – always log out.
- Regularly change your password