# Operating Systems Security

* The security of operating systems has always been a concern for users, and especially so with the invention of the Internet.
* Operating system developers are constantly creating new ways to protect computers from hackers.
* The three most common operating systems are Linux, Mac OS and Windows, each having a different set of security features.
* Determining which of these operating systems is the most secure from hackers is not easy as there are many factors that must be taken into consideration.

# Common Operating Systems

## Windows

* There are two releases currently in use today. Windows XP, released in 2001, is currently on 79.07% of all personal computers in the world 1. Windows Vista, released in 2006-2007, has a market share of 7.97%.
* Windows provides a fairly straightforward system that is useful to a beginner and a more advanced user.
* It is a closed source operating system, so only the developers have access to the source code of Windows.

## Mac OS

* The most recent release is the Mac OS X. It is very different from the original Mac OS, having an improved GUI and many more features.
* Its market share is estimated to be from 6% to 13% in the personal computing markes.
* It is also meant to be easy to use and also have advanced features. It is a mainly closed source operating system but some major components are open source.

## Linux

* Linux, in general, is a more advanced operating system.
* Although it often has a point-and-click interface, some things must be done via a command line, making it slightly harder to use.
* For this and several other reasons, this operating system is better suited for someone more knowledgeable in computers.
* It is a completely open-source operating system, meaning anyone can view the source code[3].
* It also has many different distributions.
* Each distribution focuses on different features such as speed, ease-of-use or security. The Linux market share is approximately 1% .

# Security Features

## Windows Security Features

* Vista, will be the focus here since it is the newest. Some of the more major security features include the following:
  + User Account Control
* An example of User Account Control‎
* Each time the something occurs that may affect the systems security, a prompt will appear that asks whether or not it should be allowed.
  + Address Space Randomization
* Many hacker exploits involve overflows into other portions of system memory in order to manipulate certain pieces of code. Vista has randomized memory in order to prevent this. By having memory more scattered, overflows often will not modify the correct address in memory, thereby preventing an exploit.
  + Integrity-Level Access
* Everything that is running in Vista is given a certain trust level. For example, something with lower trust cannot modify something with a higher trust level, but something with higher trust may be able to modify something with a lower trust level.
  + Improved Firewall and Address Stack
* Some updates and improvements from the XP firewall and network security.

## Mac OS X Security Features

* Mac OS X Leopard is the most recent release of Mac OS X. Some of its major features are:
  + Open and Closed Source
* Since a portion of the operating system is open source, faults in some of the code can be found by anyone. However, most of it is closed source. This mix of open and closed source aids in security as you get obscurity as well as some freely available code.
  + Sandboxing
* Gives programs as few resources as possible so as to prevent the program from gaining access to vital areas of the system.
  + File Tagging and Signed Applications
* If a program has not been run before, it is tagged. The first time it is opened, the user is asked if the file is OK to be run. Signed applications are ones that have a digital signature. These help identify the integrity and trustworthiness of the program.
  + Library Randomization
* Same idea as the Windows address space randomization, this helps protect against exploits.

## Linux Security Features

* The number of Linux security features differs with each distribution. Some of the most notable general features are:
  + SELinux
* Provides mandatory access control and integrity checking of programs and processes.
  + Open Source
* Some believe that being open source gives Linux a major advantage security-wise. Instead of just developers fixing bugs, all users are capable of this. Although this may not always guarantee security, it has worked fairly well so far.
  + Stack Smash Protection, Buffer Overflow Detection, Exec-Shield
* All of these are systems to prevent exploits. Exec-Shield provides address space randomization, while the others are specific features designed to detect specific exploits.

# Types of IT Security Software

* How does IT security software work?
* In essence, it detects and, in some cases, mitigates security attacks in your system.
* Since there are various types of security attacks, there are also various types of security products to target each one of them. Here are some of the most popular ones:

Firewall

* The over-arching term “firewall” refers to the specialized defense systems for a single computing device or computer network.
* It filters data that enters or leaves a computer or network by blocking or restricting network ports from viruses and hackers.
* It also serves as a barrier between a trusted and untrusted network by only allowing traffic that’s defined by the firewall policy to enter the network.
* Serving as your computer’s first line of defense, this utility also comes in even more various types such as proxy firewall, stateful inspection firewall, unified threat management (UTM) firewall, next-generation firewall (NGFW), and threat-focused NGFW.

Antivirus

* This software utility is designed to prevent, search, detect and remove malicious software or malware such as viruses, worms, scareware, and Trojans.
* With the constant onslaught of new viruses, these programs are often updated to enable the system to check new threats.
* While vendors vary in their offerings, some of its basic functions include scanning files and directories for suspicious patterns, scheduling automatic scans, scanning of a specific file of your computer, CD, or flash drive at a given time, removing any detected malicious codes or infected files, and providing you an overview of your computer’s health.

Spyware detection

* Spyware, also called malware and adware, are software programs installed on your computer without your consent.
* Anti-Spyware software is used to detect their presence on your computer or network and prevent or remove their installations.
* Removing them is crucial because they “spy” and record your personal information from your computer, as well as computing behaviors such as your documents, web browsing, and keystrokes.
* This can tailor the advertising on your computer, change its configuration, and even send your personal details to another remote computer.

Password protection

* One of the highly used methods to prevent unauthorized access to a computer, file, folder, and system is protecting it with a password.
* The challenge of having a password lies in human memory. In most cases, many people use an easy-to-remember password such as birthdays and family names (and in many cases, the word “password” itself) which also makes it easy to guess for cybercriminals.
* Furthermore, many reuse the same password across various platforms which exposes risks to all your accounts even when only one is compromised.
* This is where password protection security comes in handy in generating strong passwords and storing them securely.

# Benefits of IT Security Software

Prevention of viruses, spyware, and identity theft

Hackers are finding trickier ways to create viruses that may pose as anti-virus software, email from a friend, or imposter bank websites. Once they infect your computer, they can drastically slow down your processing speed, delete critical data, and damage your computer or network systems.

Protection of valuable information

Information is one of the most valuable assets of any organization. Hence, its protection is a vital part of your IT infrastructure. Loss of critical information caused by data corruption can be detrimental to your business.

Ensure compliance

Many IT departments need to comply with legal, insurance, and industry restrictions to perform the management and transmission of data. Some of the most notable regulations to take note of includes FIPS, PCI/DSS, Gramm-Leach Bliley, HIPAA, and FISMA.

Security for clients

Give your clients peace of mind by making them aware your system is protected. At a time where cybersecurity is crucial, this benefit potentially increases your sales and marketability. The security and safety of their sensitive personal information are some of the customer’s primary concerns which make them hesitant to share their information and make transactions online.

Reduced costs of development

Implementing a security solution early on prevents you from high costs along the way. While it’s never too late to install security software in your system, the sooner you have it, the better. If you choose to do it later, you’ll have more codes to modify.