Open Source versus Closed Source Operating Systems
Which is the most secure ?

What does proprietary/closed source mean ?

In computer science, when a program is proprietary or closed source, **its source code is not accessible**. This means that no one, except for the owner and developer of the program (e.g. Microsoft® for Windows™) can see and modify it.

In terms of security, this means that even if there are breaches in the system, they are hard to find because of a security concept called **"security by obscurity"**.

What is an Operating System (OS) ?

An Operating System, or OS, is software always running on a computer. It **manages the computer's resources** (memory, video, CPUs ...) and **provides an interface for a programmer between the hardware and a program** via a special kind of program called a **kernel**.

A kernel should be secured, because **it allows programs to access the material and should prevent them to behave not like they should**. Sometimes, a breach is found, that is to say a certain type of code can cause the program to have full access to the machine and do whatever it wants. This is due to a **kernel vulnerability**.

What common people see as an OS is the User Interface, with windows, menus, etc. But that kind of interface isn't required for an OS to work: a command line is quite powerful too!

What does open source mean ?

A program is called Open Source when **its source code is accessible to anyone**. That means that once you accessed the source code, you can **read it**, **modify it**, and **get your new version to work** by an operation called compilation.

In terms of security, this means that if there are **breaches** in the system, they **are visible to anyone**, and the source code can be **edited by anyone to correct this breach**.

Microsoft® Windows™

First release: November 20 1985 (Windows™ 1.0)

Main Uses: Personal Computer, Server, Super Computing, Mobile, Embedded devices

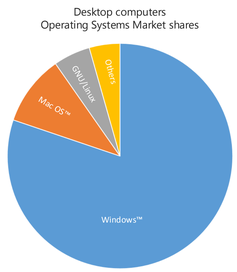
Windows™ is the most used OS on personal computers, because Microsoft® has many contracts with manufacturers for them to preinstall Windows on their computers.

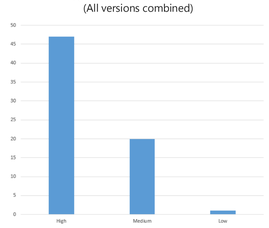
Windows™ can also be found on **smartphones and embedded devices** and is known to be quite stable and lightweight on such devices.

Due to the **massive use of Windows™** everywhere, it has been the **target of plenty of hackers, malwares, viruses, Trojans and other bad things**. These programs uses programs or OS vulnerabilities to gain a full access to the machine.

68 vulnerabilities in 2014

Security Updates: weekly (every Friday)





Apple® Mac OS X™

Search Polytech

First Release: January 24 1984 (System 0.0) September 13 2000 (OSX™)

Main Uses: Personal Computer, Mobile.

Mac OS™ is a popular OS running exclusively on Apple® computers. It is also preinstalled on the machines, as **Apple is both the developer of the hardware and the software**.

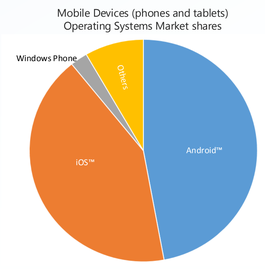
Mac OS™ can also be found on **smartphones**, as iOS and Mac OS share some source code. The iPhone is quite popular !

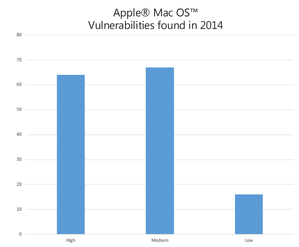
Plenty of Apple® users think that they are free with malwares, but the truth is as Apple is gaining market shares, the number of found vulnerabilities tends to increase as well.

Note: the **kernel** that Apple created and uses, called **Darwin, is Open Source**. All **the rest of the OS is closed source**.

147 vulnerabilities in 2014

Security Updates: every one to three weeks





GNU/Linux

root@localhost ~#

First Release: October 5 1991 (Version 0.01)

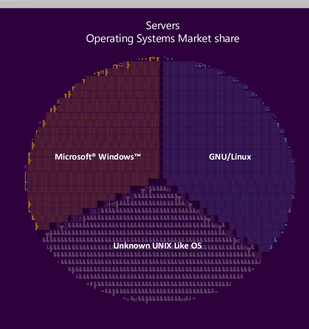
Main Uses: Server, Personal Computer, Mobile, Embedded, Supercomputing.

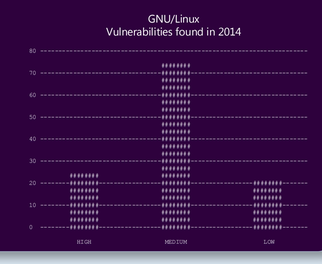
GNU/Linux is the most used OS on servers. It was created by Linus Torvalds, and **is managed by The Linux Foundation** and it is preinstalled on some machines. **Many GNU/Linux versions exists, called distributions**, providing the kernel and a set of programs.

GNU/Linux can also be found on **smartphones**: **Android uses a GNU/Linux kernel**.

119 vulnerabilities in 2014

Updates as soon as the vulnerability is fixed: via package manager (usually within 1 hour to 3 days)





Conclusion

As a conclusion, we can say that **"security by obscurity" isn't effective at all**. Even if the source code is closed, some techniques exists to **analyze code and find vulnerabilities**, but the **Open Source world isn't breach-proof**: GNU/Linux has suffered from important vulnerabilities in 2014, like Heartbleed and Shellshock.

The main difference here is **the delay between the vulnerability's discovery and the update publication**: in the **closed source world, users are dependent of the company** that publish them whereas in the **Open Source world everybody can work on a solution**, publish it, get it approved and deployed on user systems very quickly. But **the Open Source project has to be popular** for the community to care about vulnerability of the software.