Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.106 – 113

SURVEY ARTICLE

SECURITY SURVEY OF FAMOUS OPERATING SYSTEMS

Muhammad Waqas
Department of Computer Science
University of Lahore
Sargodha Campus, Pakistan
hwr44ever@yahoo.com

Maria Iram
Department of Computer Science
University of Lahore
Sargodha Campus, Pakistan
merum2@gmail.com

Rehamat-E-Bari Wajeeha
Department of Computer Science
University of Lahore
Sargodha Campus, Pakistan
jiyathegeek@yahoo.com

ABSTRACT

As the computer industry advanced so much and it has more complexities, Operating System responsibilities has increased, and give challenge to the operating system developers to build a secure operating system. In this paper we will see operating system security issues computer industry has faced in desktop and mobile area. And we are proposing a general idea to improve all operating systems for security.

INTRODUCTION

Computer has improved marvelously in recent years; it has become necessity of everyone from just a scientific tool so that improving security of is an issue to the users. For this purpose Operating System plays a vital role in security of a system. Today we don't call a system by its manufacturer name but we call it by it operating system as MAC PC or Windows PC. Building a secure operating system has been and still is a major issue.

Operating system are becoming more dynamic day by day to utilize the full capacity of hardware's, as Operating system is becoming more dynamic Operating System faces some challenges which are still to be conquered. One of major challenge is security of Operating System. Informally, security is, keeping unauthorized entities from doing things you don't want them.. This will help readers to have an overview of previous work has been done for Operating System security and give a direction to start their own study and will provide help for developers to keep these security issues in mind in development of operating system. We have a lot of different kind of operating system in the market but we will analyze most famous operating system because these are used in large number publicly. Figure 1 and figure 2 are showing popularity chart which distinguish operating system and show us the market share of operating system in their respective area like Desktop operating system and Mobile operating system.

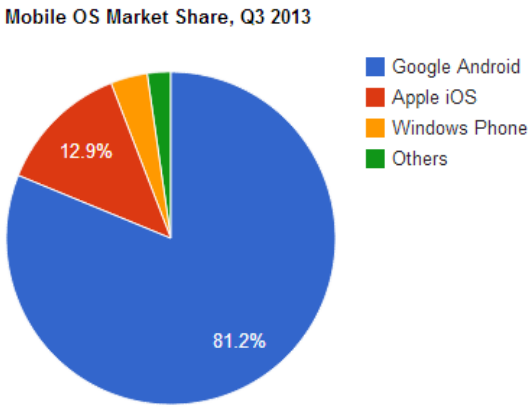

Figure 1 [4]

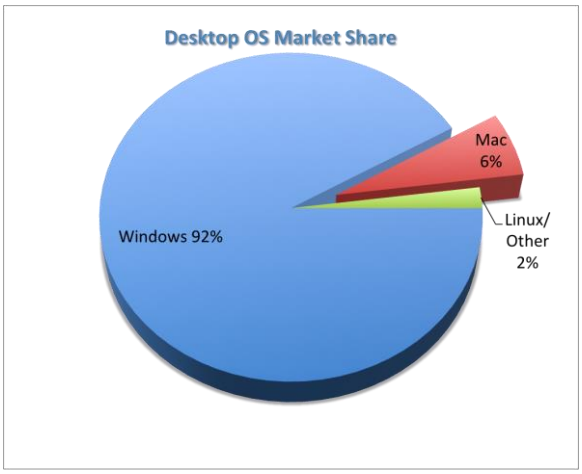

Figure 2 [5]

SECURITY

Security has been and still remains a major concern for Operating system developers and users alike. Informally security is keeping unauthorized entities from doing things you don't want them to do. Its operating system job to provide security against unauthorized users. Computer security is defined by three attributes, Confidentially, Integrity, Availability. Confidentially is prevention of unauthorized disclosure of information. Integrity is prevention of unauthorized modification of information, and Availability is the prevention of unauthorized withholding of information or resources. Operating system can provide sandbox, hashing password to protect against threats. In this paper some former researches techniques are used and we are going to explore more techniques and suggest the ideas for making a better security for Operating System.

Literature Review

SECURITY HAS BEEN IMPROVED RECENTLY BUT STILL THERE ARE FLAWS. REASONS ARE:

a) ONE REASON OF THIS THAT MOST ATTACKS ARE NOW A DAYS PUBLICLY ANNOUNCED AND DESCRIBES IN DETAIL ON INTERNET.

b) ANOTHER REASON IS THE VENDOR'S ATTEMPT TO OFFER BACKWARD COMPATIBILITY WHICH LEAVES OPEN OLD WEAKNESSES IN THE SYSTEM.

MOBILE OPERATING SYSTEMS:

Mobile operating systems combination of personal computer and managing all hardware and optimizes. Many Mobile operating systems can be seen in the market but two famous mobile systems now days are iPhone Operating System (iOS) and Android.

i. iOS

iOS derived from OS X that share by darwing foundation [1]. iOS mainly use for the iPhone and iPad manufactured by Apple. There are 4 abstraction layers in iOS which are Core Services Later, Media Layer, Core

OS layer and Cocoa touch layer. Core OS layer lies on the hardware and is the bottom layer. This layer function is to provide services including low level network access to external accessories and common operating system such as handling file system and memory management policy. Media layers contains audio, video and graphics geared towards creating the best multimedia experience on mobile device. Technology layer is for the ease of application builders that would look great. Cocoa Touch layer define the basic infrastructure and to support multitasking, touch based input, push notification and many high level notifications. This is the key framework for building iOS application.

ii. **Android**

Android Operating System is an open source and source code release under Apache license by Google. The OS is a linux based and the application software running on an application framework which includes Java compatible [2] libraries based on Apache Harmony.

Mobile Security Requirements:

Here we are discussing 5 security requirements of mobile operating system which are:

1. **Application Sandboxing**

Sandboxing is mechanism for program to run separately, it is uses to limit the app boundary. When an app is build the permissions are assigned which cannot changed dynamically on run time by application or operating system kernel. Resources can be shared but these apps will never go beyond their defined limits which are declared at startup. In iOS all application shares same sandbox but in Android every application has its own sandbox.

2. **Encryption**

Encryption is the most effective method to secure data. Encryption is a technique to convert data into a secret code so data can be secure for this purpose encryption algorithm is made and applied to data. You must have a secrete key or password to decrypt data which is an encrypted file. When encryption is not applied to text it is simple plain text and when encryption is applied to data is is called as cipher text. Encryption introduced to android in Android 3.0 Honeycomb version, first encryption method for Android is device encryption API which was released in Ice Cream Sandwich 4.0. Android applies encryption on disk level.

Encryption is also applied to iOS which was introduced in iPhone 3GS version. iOS applies hardware level encryption on data while.

3. **Memory Randomization**

Memory randomization is a process where the memory application shared library and other in a device is located randomly, this technique is important to avoid attack on the memory of running application from any malicious code or virus. This technique is applied in iOS 4.3 version and later while in Android its applied in Jelly Bean 4.1.1 and later versions.

4. **Built-in Antivirus**

In general 3 there are 3 types of popular malware that affects mobile such as Virus, Spyware and Trojan[3]. A virus is a malicious code which usually transmitted through email. Spyware is a program which collects the information about users without letting them know about it. Trojan is a desirable function but actually the purpose of the Trojan is malicious. Android and iOS both were introduced with built-in antivirus features to avoid viruses, spyware, and Trojans. Thousands of application can be downloaded from Google play safely because antivirus feature is not on android device but on Google Play [5]. It means any app downloaded except from Google Play can be very risky. We can download antivirus's applications from Google Play to avoid popular malware that affects our operating system.

In iOS there is not need of antivirus because there is no room for virus to get into the system. In iOS there is only one place to download application into the system that is App store, where every application is checked rigorously to make sure that it does not contain any kind of malicious code.

5. **Data Storage Format**

Disk Storage is a place where all the data is stored in build in storage or external storage. It is important to secure the storage to make sure your data is secured from any unwanted code. Commonly device has both internal and external storage. In Android the data can be store in both storages which in internal and external. Android implements standard crypto libraries to secure storage but it is as efficient as a password is applied. With the root access any unwanted code can access the files without any restriction and can spread malware.

While in iOS devices does not have external storage or memory but built-in storage. This requires permission to access the data. Data protection APIs in iOS are combined with passphrase which provide an additional layer of data protection. So iOS storage will be more secure than Android and make the application difficult to access the data from internal storage.

A Quick Comparrison of Android and iOS

A Quick Comparrison Of Android And iOS

Feature	Android	iOS
Sandbox	Every Application has its own Sandbox	All application shared same sandbox
Encryption	Encryption is on Disk Level	Encryption is on hardware level
Memory Randomization	Applied in 4.1.1 versions and later versions	Applied on 4.3 and later versions
Buit-in Antivirus	Antivirus can be downloaded from Google Play, virus checking is done on Google Play only, can be easily attacked because no built-in antivirus, any application outside from Google Play is risky	No antivirus needed because application can be downloaded only from Apps store and checking been done in Apps store.
Data Storage	Have an external storage and it can be access by unwanted code.	No external storage which makes difficult for the unwanted code to access built-in storage.

By this comparison we conclude that iOS security is better than Android system.

DESKTOP OPERATING SYSTEM

Many desktop operating system can be seen in market but here we are going to discuss two most famous and in most use desktop operating system which are Windows and Mac.

Windows

Microsoft windows are the most popular and most used operating system in the world. It's a graphical series of operating system of Microsoft. As figure 2 shown above MS Windows dominate 90% of desktop operating system shares. Microsoft Windows is a closed source operating system.

- **Windows 9x**
- **Windows XP**
- **Windows Vista**
- **Windows 7**
- **Windows 8**
- **Windows 8.1**

Windows Security

As the Microsoft windows is the most used operating system it has more threats than other operating system as well. In 2005 over 1000 new viruses and worms were seen in six months duration, and 11000 malicious programs, viruses, Trojans, back-doors and exploits were written for windows. Microsoft windows have released a lot versions and every operating system has some security issues.

User Space and Kernel Space
The Windows operating system is designed to support applications by moving more functionality into the operating system, and by more deeply integrating applications into the Windows kernel. Which doesn't have separation between user space and kernel space? Which may cause the critical damage to Kernel?
Update
Microsoft doesn't want to spend money on previous versions of windows, they don't provide windows update instead they are improving their flaws in upcoming versions.
Firewall
It only restricted inbound traffic and did not provide any mechanism for blocking or filtering traffic outbound from the Windows PC.
Hidden File Extensions
Windows continues to hide known file extensions by default. In other words, rather than displaying a full file name like 'pcworld.docx', Windows will only display 'pcworld'.
The idea is to make things more simple or user-friendly. We don't want to confuse the end-user with frivolous details like 'docx', or 'xls', or 'mp3'.
Internet Explorer
The security flaw allows attackers to slip malicious code into an website, using a compromised file. When a victim visits the tainted website using any of the Internet Explorer web browsers versions 6 through 11, attackers could gain full user rights over the victim's computer and potentially all information on it.
Adobe Flash Player
Gain access to a system and execute arbitrary code user privileges.
Memory
This problem was very common in windows 9x family and windows xp, although windows xp has made a lot improvements over windows 9x, but they both share this memory problem, when any user program try to access the operating system memory or other user program it result come in memory dump and gets crashed.

MAC OS
MAC OS is second most popular and widely used operating system which share 6% of desktop operating system market share as shown in the figure 2. It is UNIX based graphical user interface operating system made only for MAC computers by Apple Inc.

MAC Security

MAC is second most popular operating system, so there are not too many viruses for MAC. But it doesn't mean MAC doesn't need security. Recently a Trojan name variously Mac Protector, Mac Defender and Mac Guard showed on Apple machines, a window claiming to be the Apple Security Center pops up and indicates that virus has been found on this computer, and then it prompts to user to download Mac Protector and this software intended to steal credit card information [6].

When installing Mac OS X 10.5 Leopard, destination volumes may not appear in the installation window for a while, even though the volumes are visible while started from Mac OS X 10.4 or in Disk Utility.

After performing an upgrade installation the default type of Mac OS X 10.5 Leopard, an administrator account may change to a standard one.

After installing Mac S X 10.5 Leopard on a 20-inch or 24-inch iMac(mid2007) computer (ones that have an aluminum frame), user may not be able to log in at login windows, login name and password are apparently accept but after a blue screen appears for a few seconds, the login windows reappears instead of your desktop.

After installing Mac OS X 10.5 Leopard user may not be able to log in to account that has no password which was used in Mac 10.2.x and migrated to Leopard.

Linux

In Linux security system has two parts:
1. Authentication
2. Access control.

Some security issues regarding Linux operating system
Local Security
Local users create a lot of problems for system. It is bad policy to provide accounts to people you don't know or for whom you have no contact information. It is better to follow some rules of thumb when

offering access to your Linux machine: give users minimum privileges monitor when and where they log in, remove inactive accounts and prohibit the creation of group user IDs.

Root Security
The root account has authority over the entire machine; you should use it only for specific tasks. Even a small mistake made while logging in as a root user can lead to significant problems. Follow the simple rules below and they will help you.

• When running complex commands, first run them in a non-destructive manner. A simple example is to do an 'ls' before doing an 'rm' so that you are sure about the files you are going to delete.
• Give users an interactive rm for deleting the files.
• Become 'root only' to do specific tasks. If you want to experiment with something, go back to a normal user shell.
• The command path, which specifies the directories in which the shell searches for the programs, is very important. Limit the command path and never include '.' (signifying the current directory) in your command path.
• The /etc/securetty file contains a list of terminals that root can log in from. Be careful while adding an entry to this file.
File Security (Virtual File System allows Linux to support many different file systems, each presenting a common software interface to the VFS)
Keep in mind the following points to help protect your systems and data stored on them.
If you are exporting file systems using NFS, configure /etc/exports with the most restrictive access possible. Do not use any wild cards. Their integrity needs to be maintained, as they help in determining when and from where a user has entered your system.
World-writable files can serve as a security hole. Also, world-writable directories are dangerous as they allow an intruder to add/delete files. You must locate the world-writable files on your system and make sure that you know why they are writable.
It is also important to locate the unowned files. The presence of unowned files might also be an indication that an intruder has accessed your system.:
Before you change the permission on any system files, make sure you know what you are doing. NEVER make changes to the permission on a file just because it is the easy way to get things working.

- Memory management
- Buffer Error (buffer overflow)
- Page Fault Handling
- Configuration errors
- Information leak
- Race Condition
- Resource management errors
- Input Validation
- Password Security

File permissions
make sure that your system files are not open for casual editing by users and groups who do not have the appropriate permissions.
The Linux operating system distinguishes the access control based on three characteristics: **owner, group and other**. Access to a file will be determined by permission bits and these bits are 'rwx' – where 'r' identifies 'read', 'w' identifies 'write' and 'x' identifies 'execute'. We can set or reset these three permission bits based on the kind of access that we are interested in giving to a user. This is considered as a basic level of preventing access to a file from unauthorized sources.

Integrity checking
There is a very good mechanism to detect local attacks on your system. This is referred to as 'integrity checking'. Tripwire, Aide and Osiris are some of the popular integrity checkers. These integrity checkers will run a number of checksums on all important binaries and configuration files and compare them against a database of former, known values as a reference. Thus any changes in files can be easily flagged. Based on these signals, a system administrator can make appropriate changes so that integrity of important files is maintained.

Password security

Most Linux distributions come with 'passwd' programs that do not allow you to set a password that can be easily guessed. Thus, it is necessary to make sure that your passwd program is up to date. Linux uses a one-way encryption algorithm known as DES (Data Encryption Standard), which is used to encrypt your passwords. The encrypted password is stored in /etc/passwd. When you try to log in, the password you type again gets encrypted and is compared with the entry in the file that stores your password. A match means you have entered the same password and you are given access to the system.
Shadow passwords are a means of keeping your encrypted password information secret from the normal users. Recent versions of both Red Hat and Debian Linux use shadow passwords by default. Shadow passwords are saved in /etc/shadow and they can be read only by privileged users.

Kernel security

As the kernel controls your machine's networking, it is essential to keep it secure. Let's look at some popular kernel configuration options that relate to security.

IP forwarding: If you enable IP forwarding, your Linux box becomes a router. You can enable or disable IP forwarding by using these commands:

root# echo 1 > /proc/sys/net/ipv4/ip_forward /* for enabling */

root# echo 0 > /proc/sys/net/ipv4/ip_forward /* for disabling */

IP firewalling: This option is very useful if you want to protect your dial-up workstation from someone entering via your PPP dial-up interface.

IP firewall packet logging: This option displays the information about the packets your firewall receives.

Other security implementations

The one to consider here is the implementation of IPSEC for Linux. IPSEC is a mechanism to create cryptographically secure communications at the IP network level. The main idea here is to provide authentication, integrity, access control and confidentiality for your information.

Security guidelines

Among all the concerns surrounding the writing of good code, security necessarily comes at the top. Security problems can come from people actively trying to penetrate your security or from simple issues such as someone providing unexpected inputs to a program or running some wrong commands. Too much access to systems can mean that users – even with legitimate access – can cause trouble, either accidentally or on purpose.

REFERENCES

[1] Ahmad, M.S.; Musa, N.E.; Nadarajah, R.; Hassan, R.; Othman, N.E., "Comparison between android and iOS Operating System in terms of security," *Information Technology in Asia (CITA), 2013 8th International Conference on* , vol., no., pp.1,4, 1-4 July 2013
[2] Khadijah Wan Mohd Ghazali, Rosilah Hassan and Zulkarnain Md Ali, A Network Device Simulator, IEEE ICACT 2013, PyongChang Korea Jan 27-30, 2013, pp.378-381
[3] Qing Li; Clark, G., "Mobile Security: A Look Ahead," Security & Privacy, IEEE , vol.11, no.1, pp.78,81, Jan.-Feb. 2013 doi: 10.1109/MSP.2013.15
[4] http://i0.wp.com/blog.goyello.com/wp-content/uploads/2014/01/2014-01-23-13_15_18.png
[5] http://www.laridian.com/images/2013-04%20Desktop%20OS%20Market%20Share.png

[6] http://computer.howstuffworks.com/macs/10-differences-between-macs-and-pcs.htm#page=9
[7] G OLDBERG, R. P. Survey of virtual machine research. IEEE Computer Magazine (June 1974), 34–45.
[8] B HARGAVA, R., S EREBRIN, B., S PADINI, F., AND MANNE, S. Accelerating two-dimensional page walks for virtualized systems. In ASPLOS ’08: 13th intl. conference on architectural support for programming languages and operating systems (2008)
[9] B EN-YEHUDA, M., M ASON, J., X ENIDIS, J., K RIEGER, O., VAN DOORN, L., NAKAJIMA, J., M ALLICK, A., AND WAHLIG, E. Utilizing IOMMUs for virtualization in Linux and Xen. In OLS ’06: The 2006 Ottawa Linux Symposium, pp. 71–86.
[10] L EVASSEUR, J., U HLIG, V., S TOESS, J., AND G ¨ OTZ, S. Unmodified device driver reuse and improved system dependability via virtual machines. In OSDI ’04: 6th conference on Symposium on Operating Systems Design & Implementation (2004), p. 2.
[11] I NTEL CORPORATION. Intel 64 and IA-32 Architectures Software Developers Manual. 2009.
[12] S UGERMAN, J., V ENKITACHALAM, G., AND LIM, B.-H. Virtualizing I/O devices on VMware workstation’s hosted virtual machine monitor. In USENIX Annual Technical Conference (2001).
[13] RUSSELL, R. virtio: towards a de-facto standard for virtual I/O devices. SIGOPS Oper. Syst. Rev. 42, 5 (2008), 95–103.
[14] L IU, J. Evaluating standard-based self-virtualizing devices: A performance study on 10 GbE NICs with SR-IOV support. In IPDPS ’10: IEEE International Parallel and Distributed Processing Symposium (2010).
[15] R AM, K. K., S ANTOS, J. R., T URNER, Y., C OX, A. L., AND RIXNER, S. Achieving 10Gbps using safe and transparent network interface virtualization. In VEE ’09: The 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (March 2009).
[16] Y ASSOUR, B.-A., B EN-YEHUDA, M., AND WASSERMAN, O. Direct device assignment for untrusted fully-virtualized virtual machines. Tech. rep., IBM Research Report H-0263, 2008.
[17] Bounding the Running Time of Interrupt and Exception Forwarding in Recursive Virtualization for the x86 Architecture, Wing-Chi Poon (VMware) Aloysius K. Mok (UT Austin). Technical Report VMware-TR-2010-003 Oct 20th 2010 VMware, Inc.
[18] Aloysius K. Mok, Alex Xiang Feng “Real-Time Virtual Resource: A Timely Abstraction for Embedded Systems”, Proceedings of the 2nd International Conference on Embedded Systems, October 2002, pp.182-196.

