IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VII (Nov – Dec. 2014), PP 64-67
www.iosrjournals.org

Security Evaluation of Google Chrome Operating System

Godwin Okechukwu Ogbuabor
Department Of Computer Science, Michael Okpara University of Agriculture, Umudike

Abstract: *Due to the increase nature of computer threats and attacks, the security of the operating system is paramount in the computing world today. Every modern computer system, from network servers, workstation desktops, to laptops and hand-held devices, has a core piece of software, called operating system (OS) executed on the top of a bare machine of hardware that allocates the basic resources of the system and supervises the execution of all applications within the system. This paper investigates and evaluates the security of Google Chrome Operating System. Google Chrome Operating system is an operating system developed by google, which runs on specialized hardware. The Chrome OS differ from traditional operating system such as Windows in that it is designed to work specifically with web applications. In this operating system, the user data lives essentially on the web. Thus, if the physical machine-laptop is lost or stolen, the user can still access their data online. However, the Chromebook also allows users to access downloaded data offline, which must be kept safe. To achieve this, Chrome OS ensures that all downloaded data is protected and that code running on this Chromebook is safe to use. In order to avoid security challenges of traditional operating system such as virus and worms, ChromeBook not only ensures that the code is safe, but also incorporates an autoupdate features to add new patches to the system.*

Keywords: *Security, Google Chrome, Web, Operating System,*

I. Introduction

The Internet has become a central part of the computer experience. Before the Web caught fire in the late 1990s, home computing was largely a singular experience. Computer users create documents on a PC and save those files to a hard or floppy disk, or work within a local Area Network in an office (Chandler, 2010).

Nowadays, computing have become a Web-centric experience, we perform many of our Internet tasks through software called a Web browser. That browser, which may be a program such as Firefox or Internet Explorer helps retrieve information from the Internet multiple times a day. "Google is trying to reshape the computer experience by using its understanding of the Web to create the new Chrome Operating system (OS)" (Chandler,2010).

An Operating System (OS) is a special kind of program that organizes and controls computer hardware and software. Operating system interacts directly with computer hardware and serves as a platform for other applications. Whether it's Windows, Linux, Unix or Mac OS, Your computer depends on its OS to function.

That is the reason of some people objection to the term Web OS. A web OS is a user interface (UI) that allows people to access applications stored completely or in part on the Web. It might mimic the user interface of traditional computer operating systems like Windows, but it doesn't interact directly with the computer's hardware.

Traditional Operating system such as Windows requires a lot of hard drive space and demand some work on our part to function. You have to install the programs you desire to use individually, manage the OS, manage device drivers and perform security update regularly.

Google embraced the concept of an ultra-simple, Web-centric OS in large part due to the huge recent success of notebooks. Notebooks are small laptop computers that are designed to let users access the Web, they are inexpensive and feature-limited hardware.

Google Chrome Operating system is an operating system, developed by Google that runs on specialized hardware (Fang et al., 2010). The Chrome OS is based on the open source project Chromium OS. This operating system differs from traditional operating systems because of its design nature- the Operating system is designed to work specifically with web applications. The underlying principle of Chrome OS is that more data is moving to the web dictates a move toward cloud computing. This implies that all of your data are stored online; in the 'cloud' to enable you access them from any computer anywhere provided that there is internet connectivity. This model will help to develop a better overall OS experience and focus on developing an OS with improved speed, security and simplicity.

Due to the crucial role of the operating system in the operation of any computer system, the security of an operating system (OS) will have fundamental impacts to the overall security of a computer system, including the security of the applications running within the system. A compromise of the underneath operating system will certainly endanger any application running within the system.

II. Related Works

An operating system is a piece of software that controls the hardware and with which applications interact in order to carry out functions (Habib and Zubair, 2009).

Google's Chrome Operating System is a web OS which is a Linux-based, open source operating system launched in July 2009, with the aim of building an operating system that provides a fast, simple and more secured computing experience (Azad,2012).

Traditional operating systems such as Windows require a lot of hard drive space and demand some work on your part (Chandler, 2010). You have to install the programs you want individually, manage OS and security updates and also manage the device drivers. Google Chrome OS aims to overhaul that paradigm.

Security of mobile operating systems was investigated by Kettula (2009) in the year 2000. The study showed that most of the mobile operating systems lack important features like permission based file access control, multi-user support and even memory protection. Mobile Operating System are used in different types of mobile devices such as Smartphones, Tablet PCs, Mobile Phones etc.

Habib and Zubair (2009) evaluated the security of Windows Mobile Operating System. The researchers stated that the problem with smartphone operating system is that a known vulnerability tends to exist for a longer time due to delayed patches, thus they can be an easy target to exploit. To expose the vulnerabilities on the network level, they carried out penetration testing on Windows Mobile 6.1 operating system. They also pointed out that Windows Mobile does offer a security infrastructure that uses security policies with code signing, but it is not impossible to bypass the security policies. The researchers concluded by saying that "while the vendors of mobile OSes have started to pay attention to OS security, these mobile OSes still have a long way to go in order to prove themselves truly worthy of the trust that is invested on them by their users today" (Habib and Zubair, 2009).

Munsee and Lee (2002) worked on Linux Operating System Security; Linux is an open source operating system that has gained much popularity. More and more people are using it for a variety of tasks

Since its birth in 1991, Linux has grown to become one of the world's most popular operating systems (Munsee and Lee, 2002). Students like it for the price and the open source flexibility. Network administrators like it because it can communicate with many other operating systems and run on virtually any processor. Internet Service Providers (ISPs) like it because of the native Internet support that it provides. Even with all the strengths of Linux, many claim that Linux isn't secure because of its open source nature. Some feel that the open source code makes it easier for attackers to find and exploit flaws in the operating system.

Munsee and Lee (2002) pointed out some attacks that are being used against Linux Operating System such as Worm Attacks, Trojan Horse Programs, Direct Physical Access or Local Hacking, Buffer Overflows etc. They narrated that attackers can easily search through the Linux code for vulnerabilities and trying to exploit them. Other systems that don't have open source are not as easily probed for flaws that can be exploited.

When it comes to commercial operating systems, the only way vulnerability can be found is through an attack, and the only way vulnerability can be fixed is through the manufacturer. Linux vulnerabilities are fixed almost as quickly as they are found. The Linux community works together, to fix problems as quickly as possible. As for other operating systems, unless the problem is major, the fix will have to wait (Munsee and Lee, 2002).

They suggested that in order to keep Linux operating system secured, we need to continue installing patches and also configure Linux completely.

III. Features Of Google Chrome Os

User Interface

Design goal for Google OS user interface involves using minimal screen space by combining applications and standard Web pages into a single tab trip, rather than separating the two. It is designed with a reduced window management scheme that would operate only in full screen mode.

Architecture

In preliminary design documents for the Chromium OS open source project, Google enumerated three-tie architecture: Firmware, browser and window manager.

- The firmware contributes to fast boot time by not probing for hardware, such as floppy disk drive that are no longer common on computers, especially netbooks. The firmware also contributes to security by verifying each step in the boot process and incorporating system recovery.
- System-level software includes the Linux Kernel that has been patched to improve boot performance. Userland software has been trimmed to essentials, with management by upstart, which can launch services in parallel, re-spawn crashed jobs and defer services in the interest of faster booting.
- The window manager handles user interaction with multiple client windows much like other windows managers.

Integrated Media player and file manager

Google integrated a media player into both Chrome OS and Chrome browser which enable users to play back MP3s, view JPEG and handle other multimedia files while offline.

Chrome OS also includes an integrated file manager which resemble those found on other operating systems. This file manager has the ability to display folders and their associated files as well as preview and manage file contents using a variety of Web applications.

Hardware Support

Google Chrome OS is initially intended for secondary devices like netbooks, not a user's primary PC, and will run on hardware incorporating an x86 or ARM. While Chrome OS will support hard disk drives, Google has requested that its hardware partners use solid-state drives due to their higher performance and reliability, as well as the lower capacity requirements inherent in an operating system that accesses applications and most user data on remote servers.

Printing

Google Cloud Print is Google service that helps any application on any device to print on any printer. While the cloud provides virtually any connected device with information access, the task of developing and maintaining print subsystems for every combination of hardware and operating system-from desktops to netbooks to mobile devices- simply isn't feasible. However, the cloud service would entail installing a piece of software, called a proxy as part of Chrome OS. The proxy would register the printer with the services and manage the print jobs, provide the printer driver functionality and give status alert for each job.

IV. Security Evaluation

The Chrome browser is the only real 'user application' running on Chrome OS with which the user interacts. All other interactions with data occur through web applications in the browser. Google chrome OS inherits the security of the Chrome browser. That is each web app is sandboxed and privilege separated so that each process runs in its own namespace. In addition, the Chrome browser provides tab isolation and isolated app storage resources.

Chrome OS also employs mandatory access control scheme on both the application and system level. Even though the chrome browser is the only user application running, the mandatory access control ensures that the browser will have access to the resources it needs from the user it is currently signed in as. This prevents different web apps from messing with each other, and if one breaks, it limits the effects.

One of the Chrome OS's major security goals is to ensure that the system is safe to use. The approach Chrome OS uses is verified boot. On boot up, Chrome OS checks that the firmware, Kernel, and system data are all valid by checking signed hashes. The other major security goal is Chrome OS pursues is keeping important information secret. Chrome OS achieves this by keeping the data in a separate partition from the root data. Each user's data is encrypted using different keys, thus user can only access his own data.

One of the main selling points of the Chrome OS is that the important data is on the cloud, and the laptop only act as a portal to it, which means losing the physical laptop is not a catastrophe (Fang,2010). However, because this is more open and connected, one may argue that is less secure than physical computers. In recent years, the numbers of attack on the web have grown rapidly. Stealing password through phishing attacks is currently easier than stealing physical hard drives or breaking the cryptography. If attackers succeed in gaining access to the user's password, the attacker can easily access all the data without even needing to have the physical computer. Due to the insured nature of the use of password and how easy it is to write attack to get passwords, (Fang, 2010) pointed out that this is a fundamental flaws of Chrome OS and potentially all cloud based systems. He argued that Chrome OS does not address phishing, which means that it does not provide any stronger guarantees about the data online.

V. Conclusion

Due to the important role of operating system in the operation of any computer systems, the security of operating system have fundamental impacts to the overall security of a computer, including the security of all applications running within the system. In fact, the fundamental security design of Chrome OS is solid; it is obvious that the system was designed with security in mind.

Unlike other operating systems, Chrome doesn't bombard someone with an endless series of OS update alerts. When you connect your notebook to the internet, Googles updates Chrome for you automatically. The whole idea is to make your computing experience easier and more secure, with less fuss and frustration.

Nevertheless, google can also improve the security of Chrome OS to handle web attack to ensure maximum security and boost confidence in the use of the operating system.

References

[1]. Azad, S. (2012). Chrome OS and System Architecture. Retrieved November 3, 2014, from http://sufianalogy.blogspot.com/
[2]. Emperador, A., & Norman, A. N. (2013). Analysing ChromeOS's Boot Performance. Austin: The University of Texas .
[3]. Fang, K., Hanus, D., & Zheng, Y. (2010). Security of Google Chromebook. Massachuset Institute of Technology Cambridge.
[4]. Habib, S. M., & Zubair, S. (2009). Security Evaluation of the Windows Mobile Operating System. Goteborg, Sweden: Chalmers University of Technology.
[5]. Kettula, A. (2009). Retrieved October 2014, from Secuirty Comparison of Mobile OSes: http://www.tml.tkk.fi/Opinnot/Tik-110.501/2000/papers/kettula.pdf
[6]. Munsee, C. L., & Lee, C. (2002). Security Evaluation of the Linux Operating System. Oregon: Oregon State University, Corvallis,.
[7]. Nathan, C. (2010, June 30). How the Google Chrome OS Works. Retrieved November 2014, from <http://computer.howstuffworks.com/google-chrome-os.htm>
[8]. Yang, C.-Q. (2003). Operating System Secuirty and Secure Operating System. SANS Institute.