ASH1925024M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:36AM (UTC-0500)

Submission ID: 1782989774

File name: ASH1925024M.pdf (263.11K)

Word count: 2719

Character count: 14435

Security measures in Windows, Unix and MacOS

Arnab Dey
ASH1925024M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security (Security measures in Windows, Unix and MacOS)**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

Abstract

Operating system (OS) security is a key component of computer security. With ransomware and spyware on the rise, enterprises need to stay vigilant to protect data from attackers. Most of us understand the need for strong passwords to protect our devices from unauthorized access. We may, however, neglect to take advantage of additional security features offered by the different operating systems. Ever wondered what your operating system does to keep your data safe? In this paper, we will discuss different security measures in Windows, Unix, and MacOS.

Keywords: Windows, MacOS, Unix, Security

1 Introduction

Operating System (OS) is software that manages and controls the main computer hardware, the hardware peripherals and software resources, so also the users [1]. It also offers the platform and support for application programs and acts as an interface between the computer user, programmers inclusive, and the computer hardware. Applications software like word processors, spreadsheets, databases, and other dedicated applications that businesses need, run on a given OS platform. Operating systems provide standard services for processes implementation such as storage, deadlock, scheduling and other processes. It also provides a programming environment that enables a user to write and execute programs in a much convenient and efficient way.

Every computer system including desktops, laptops, tablets, supercomputers, handheld and even video game consoles use some type of operating system. There are numerous types of operating systems in today's ICT world. Mac Operating System designed and owned by Apple Inc., Windows by Microsoft Inc., Linux by Community, likewise Android by Google Inc. and others [2, 3]. Varieties of Operating Systems have emerged over the years having different features and functionalities. Understanding the functionalities of each OS guides users' decisions about the OS to install on their computers. In view of this the comparative analysis of different OS becomes inevitable. Thus the need arises for a comparative analysis that will give an overview of the similarities and difference in different types of OS with the view to presenting and mapping the features of the OS with various user services. This paper presents a comparative study of three (i.e. Windows, Mac, UNIX) operating systems based on the OS features and their strengths and weaknesses [7].

The paper is structured as follows: Section 2 presents the different security measures of the operating systems and section 3 concluded the work with a future direction.

2 Methods

2.1 7 Windows security measure

2.1.1 Windows Defender Smart Screen

The Windows Defender Smart Screen can "block at first sight," according to Microsoft. It helps protect employees if they try to visit sites previously reported as containing phishing or malware, and to stop them from downloading potentially malicious files. It can also help protect against fake advertisements, scam sites, and drive-by attacks.

"This is one of multiple layers of defense in anti-phishing and malware protection strategies," Benoit said [5].

2.1.2 Windows Defender Application Guard

Application Guard offers protection against advanced, targeted threats launched against Microsoft Edge using Microsoft's Hyper-V virtualization technology. The functionality works with whitelisting: Users can designate trusted sites to browse freely. If a site is not trusted, Application Guard will open it in a container, completely blocking access to memory, local storage, other installed applications, corporate network endpoints, or any other resources of interest to the attacker.

2.1.3 User Account Control

User Account Control (UAC) protects users by preventing malware from damaging a machine, and helps organizations deploy a better-managed desktop. When this feature is enabled, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. It can also block the automatic installation of unauthorized apps, and prevent accidental changes to system settings.

2.1.4 Windows Defender Device Guard

Defender Device Guard involves driver and application whitelisting, Benoit said. The feature changes from a mode where apps are trusted unless blocked by an antivirus solution, to a mode where the OS trusts only apps authorized by an enterprise. It operates on two components: The first, kernel mode code integrity (KMCI) protects kernel mode processes and drivers from zero-day attacks and other vulnerabilities by using HVCI. The second, user mode code integrity (UMCI) is enterprise-grade application whitelisting that achieves PC lockdown for enterprises using only trusted apps.

2.1.5 Windows Defender Exploit Guard

Defender Exploit guard includes exploit protection, attack surface reduction rules, network protection, and controlled folder access. It also provides legacy app protection including arbitrary code guard, blocking low-integrity images, blocking untrusted fonts, and exporting address filtering.

"This helps you audit, configure, and manage Windows systems and application exploit mitigations," Benoit said. "It also delivers a new class of capabilities for intrusion prevention."

2.1.6 Microsoft Bitlocker

Bitlocker is a full-drive encryption solution provided natively within Windows 10 Professional and Enterprise, Benoit said. It helps mitigate unauthorized data access by enhancing file and system protections, and renders data inaccessible if the computers are decommissioned or recycled.

"This is so important–you don't want to be the guy who got blamed after the CEO's device was lost or stolen and all the data was found on the world wide web," he added.

2.1.7 Windows Defender Credential Guard

Defender Credential Guard uses virtualization-based security to isolate secrets, so that only privileged system software can access them–protecting from credential theft attacks. Enabling this feature offers hardware security and better protection against advanced persistent threats.

The overall best security practice? "Educate your users," Benoit said. "They are the ones who click on the things and execute the files. It's the toughest thing to do, but in the very end that's the thing you have to do."

2.2 5 MacOS security measure

2.2.1 Secure Your Data With FileVault

In recent versions of macOS, Setup Assistant prompts you to activate FileVault during the installation process. Those unfamiliar with the feature may avoid turning it on if they don't understand it, and those rushing through the setup process may not even notice the option [6].

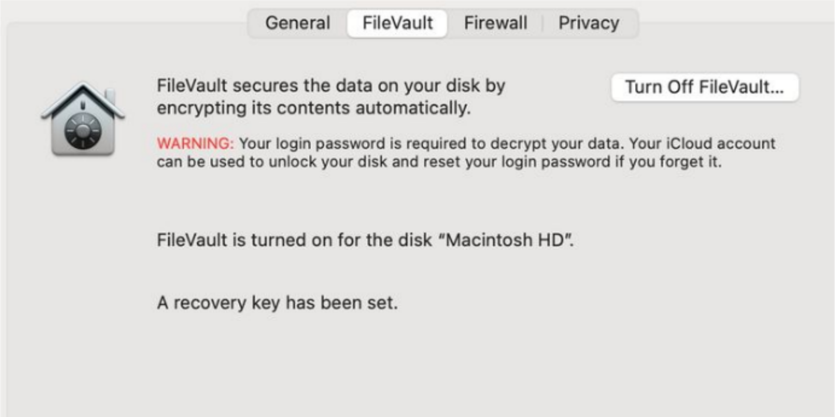
FileVault adds an extra layer of security, beyond your admin user account password, by encrypting the entire macOS volume. This means no one can access the data on your hard drive without the decryption password.

The extra protection prevents unauthorized individuals from physically accessing the contents of your computer. Without FileVault enabled, a savvy user can bypass your admin user account and help themselves to your files, as long as they have access to your drive.

Fortunately, using FileVault is a simple and effective way to increase device security and protect your data. To enable encryption, follow these steps:

1. Open System Preferences.
2. Choose Security and Privacy.
3. Select the FileVault tab.
4. Unlock the Security Padlock.

5. Click Turn On FileVault.



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: Your login password is required to decrypt your data. Your iCloud account can be used to unlock your disk and reset your login password if you forget it.

FileVault is turned on for the disk "Macintosh HD".

A recovery key has been set.

Figure 1: Filevault

If your device has multiple users, you must select Enable User for each account that should have permission to unlock the disk.

Click Continue and a prompt will appear asking how you'd prefer to reset your FileVault password if you forget it. For this, you have two options: using your Apple ID/iCloud account, or with a generated recovery key. Both options come with a warning. If you choose to use iCloud as a reset method, you should have strong security on that account. Alternatively, if you prefer to generate a recovery key, you must keep it in a safe place that no one but you can access.

Locking yourself out of an encrypted volume means erasing the entire drive to regain access, so you'll want to be diligent with your password and recovery method.

When enabled for the first time, FileVault works in the background to encrypt your drive. You should connect your device to power and allow the process to complete. Encryption time varies based on the size of your hard drive, and it's best not to interrupt the procedure. Once completed, your newly encrypted volume will make it difficult for would-be data thieves to physically access your personal information.

2.2.2 Protect Your Mac With a Firmware Password

A firmware password adds an additional layer of security to your device. When enabled, the feature prompts you for a password whenever you try to boot from an alternate volume, such as the recovery partition, attached external storage, or when using most Mac startup key combinations.

By default, unauthorized users can take advantage of certain Mac features, such as recovery or single-user mode, to tamper with your device. But a firmware password prohibits access to those areas.

Because newer versions of FileVault include similar protection measures, Apple Silicon Macs no longer require a firmware password. However, many people still have Macs with Intel chips, so can benefit from the extra security.

To set a firmware password on an Intel Mac, boot to your recovery partition by holding Cmd + R during startup and follow these instructions:

1. Click the Utilities menu.
2. Choose Startup Security Utility or Firmware Password Utility.
3. Enter a strong password you'll remember.
4. Restart your Mac from the Apple menu.

That's it. A firmware password now protects your device from unauthorized tampering and provides the ideal complement to FileVault encryption.

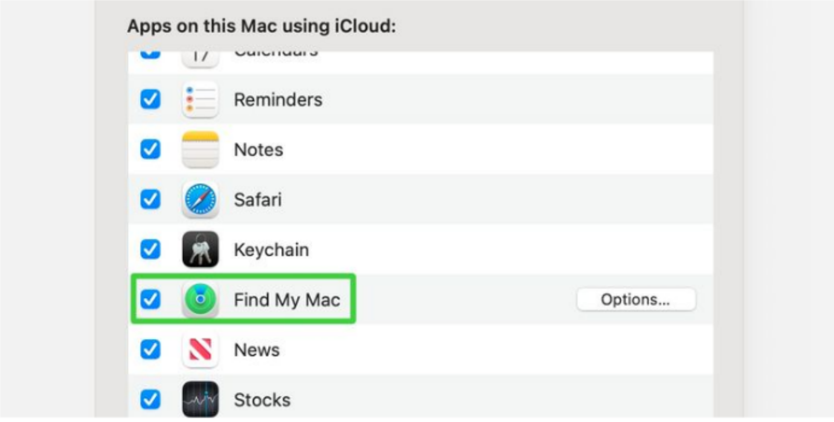
Remembering your firmware password is critical. If you forget what you entered, regaining access to your device will require proof of purchase, a trip to an Apple Authorized Service Provider, and a bill for the trouble.

This strict process ensures only the device owner can request to remove the security feature when required. We recommend noting down your firmware password in a password manager.

2.2.3 Use Find My Mac to Track, Lock, and Wipe Your Device

Find My Mac is the ultimate technological defense against thieves. The iCloud feature allows you to track your Mac if it goes missing, remotely lock your device with a firmware password, and wipe your hard drive to protect its data. You can even check the battery level of a snatched device so you know when and where it's going to lose power.

There's no good reason to avoid using Find My Mac, and setting up the feature only takes a few minutes. Here's how to configure it:



Apps on this Mac using iCloud:

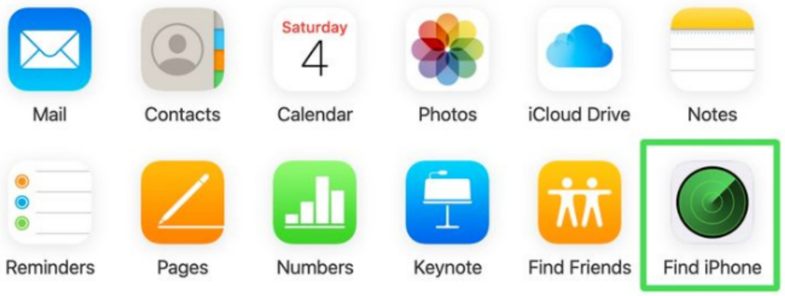
☑ Calendars
☑ Reminders
☑ Notes
☑ Safari
☑ Keychain
☑ Find My Mac
☑ News
☑ Stocks

1. Open System Preferences.
2. Choose Apple ID or Internet Accounts.

3. Select iCloud from the list.

4. Tick Find My Mac, then Allow access.

To use Find My Mac's features, navigate to iCloud.com, sign in, and choose Find iPhone. From here, you can access a list of your devices and perform the necessary actions.



Find My Mac is such an important feature because it not only helps you protect and recover a lost or stolen device, but it also deters thieves by its very existence. If more users adopt this and similar security features, stealing a computer, phone, or other protected device becomes a pointless act.

2.2.4 Apple ID Two-Factor Authentication

Enabling two-factor authentication for all your accounts, including your Apple ID, is a simple and effective way to increase security. While most people are familiar with this measure, some have yet to adopt the feature. A secure Apple ID is paramount to overall device security, as access to the account allows anyone to reset the FileVault password and disable Find My Mac.

If you haven't enabled two-factor authentication on your Apple ID, we strongly recommend you do so now. The quickest way to set up the feature is through the Apple ID panel in System Preferences. Simply choose the Password and Security option and follow the prompts.

2.2.5 System Integrity Protection

While the above tools require your activation, Apple also provides automatic security features in macOS, including System Integrity Protection (SIP).

SIP, introduced in El Capitan (macOS 10.11), prevents the root user account and malicious operators from modifying important parts of the system. The feature runs automatically and doesn't require any additional setup. With SIP in place, only Apple processes have the authority to modify system files, restricting the damage malicious operators can do if they gain access to your system.

While SIP is an automatic function, devices running a version of macOS earlier than 10.11 are missing the feature. If you're using an outdated operating system, we highly recommend upgrading unless you have a good reason not to do so. If you can't upgrade, it's probably time to replace your Mac.

2.3 3 level security measure in Unix

2.3.1 Network level

Internal kernel firewall called "iptables" - the most powerful and most integrated firewall architecture that can be in an operating system [4].

2.3.2 System level

Besides the authentication step, you ave got access level controls through permissions for each inode (that is, for example, file and directory/"folder"), where you have got users and groups of users who you can define. For each inode, you can set "user" access levels (read, write and execute), group access levels and access levels for "others".

2.3.3 White hat level

Besides the above, for most applications and servers, there is an global ongoing effort (publicly accessible and watchable) to tackle higher level of security abstraction, watching and safeguarding software exploits that surface from time to time.

3 Conclusion

Windows and Android tend to be the most widely used especially the newest versions. It is because they are affordable, secured, reliable, compatible and friendly. It could be concluded that every operating system, with a particular direction, was developed by considering targeted customers and their interest. Every Operating System, mobile OS inclusive, provides competitive and distinct features and services for their customers. However, all open sourced Operating Systems enjoys addition of new ideas, in applications and updates every day by various community developers, this also enhanced their security features and performance, while the enterprised OS lacks flexibility of design. This will not underscore the fact that every OS is good, but users' choice depends on the services required of it.

References

[1] Akinlolu Adekotujo, Adedoyin Odumabo, Ademola Adedokun, and Olukayode Aiyeniko. A comparative study of operating systems: Case of windows, unix, linux, mac, android and ios. *International Journal of Computer Applications*, 176:16–23, 2020.

[2] Brad Arkin, Scott Stender, and Gary McGraw. Software penetration testing. *IEEE Security & Privacy*, 3(1):84–87, 2005.

[3] Aileen G Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, and Monique Jones. An overview of penetration testing. *International Journal of Network Security & Its Applications*, 3(6):19, 2011.

[4] Frederick T Grampp and Robert H Morris. The unix system: Unix operating system security. *AT&T Bell Laboratories Technical Journal*, 63(8):1649–1672, 1984.

[5] Nihad A Hassan and Rami Hijazi. Windows security. In *Digital privacy and security using Windows*, pages 103–122. Springer, 2017.

[6] Laurent Marteau. Mac os x & security—an overview. *Network Security*, 2005(5):11–13, 2005.

[7] Q.R. P. A Madeup paper. *International Journal of Sample References*, 1(1):59–72, 1983. Publisher: [Wiley, Coyote Inc.].

ASH1925024M

ORIGINALITY REPORT

82%	80%	0%	42%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.makeuseof.com Internet Source	43%
2	www.ijcaonline.org Internet Source	15%
3	www.techrepublic.com Internet Source	15%
4	v1.overleaf.com Internet Source	2%
5	Submitted to University of Maryland, University College Student Paper	2%
6	Submitted to General Sir John Kotelawala Defence University Student Paper	2%
7	global.oup.com Internet Source	1%
8	www.coursehero.com Internet Source	<1%
9	explora.unex.es	

Internet Source

<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925024M

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Prep. You may be using the wrong preposition.

PAGE 3

Article Error You may need to remove this article.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 4

Article Error You may need to remove this article.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word.

Pronoun This pronoun may be incorrect.

PAGE 5

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Confused You have used **your** in this sentence. You may need to use **you're** instead.

PAGE 6

Missing "," You may need to place a comma after this word.

PAGE 7

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

PAGE 8

Wrong Form You may have used the wrong form of this word.

Confused You have used **an** in this sentence. You may need to use **a** instead.

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

PAGE 9