Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

A Comparative Study of Modern Operating Systems in terms of Memory and Security: A Case Study of Windows, iOS, and Android

Abdullahi Umar Umar[1*], Abubakar Wakili[2]
[1]Department of Computer Science, Sule Lamido University, Kafin Hausa, Nigeria
[2]Deptment of Computer Science, Jigawa State College of Remedial and Advanced Studies, Babura, Nigeria
umar.abdullahi@slu.edu.ng[1*], wakiliabubakar14@gmail.com[2]

[*]Corresponding Author

Abstract

Modern computer systems have an operating system, which serves as an interface between the device and the user and has the dual objectives of making the device easier to operate and making optimal use of device resources. The operating system offers some level of computer security like user authentication, file permission, firewall, encryption etc., but occasionally, problems develop due to societal or technical challenges like: vulnerable to malicious programs and viruses, which can cause the system to become sluggish or malicious actors be able to have an access to confidential user data, which compromise computer security. This comparative study provides insight into each of these operating systems and their relative strengths and weaknesses. The paper begins by discussing the concepts of memory management and security in general and then examines the specifics of each OS's memory management and security features. A case study of three popular applications is presented to illustrate how memory management and security features can be used in practice. The results of the comparison show that while each operating system has its own advantages and disadvantages, Windows is generally the most powerful and secure of the three, while iOS and Android offer more flexibility and ease of use.

Keywords: *Windows, operating system, Android, and iOS.*

1. Introduction

An operating system is a set of programs that manage the hardware and software resources of a computer. It provides an environment for the execution of application programs, and it provides the user interface for the user to control the computer. Common examples of operating systems include Microsoft Windows, macOS, and Linux.
It offers a setting in which a user can run programs. An operating system's primary objective is to make computers easy to use, and its secondary objective is to maximize the utilization of computer hardware (Mei and Guo, 2018). One of an operating system's primary functions is resource allocation and control, computer users should be provided with equitable access to system resources such as CPU time and memory, ensuring that no one user has greater access than any other (Bellovin and Smith, 2002).

Patches and updates for users and administrators are the main issues with operating systems. The operating system suppliers are releasing more patches, some of which necessitate restarting the entire system (Baumann *et al.*, 2007). Mobile computing has become common in our daily lives in the modern day. Mobile device operating systems must effectively optimize memory management, security, and performance because our daily activities are solely dependent on them. The three operating systems for mobile phones—Android, Windows, and iOS (iPhone OS)—each have their unique methods for allocating system resources (Awan *et al.*, 2017).

Many different embedded operating systems have been developed to meet the needs of many sophisticated industrial applications. Super loop, cooperation, and real-time operating systems, which were utilized in industrial applications, have been taken into consideration while evaluating embedded operating systems. (Hee *et al.*, 2021).

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Numerous long-term enhancements have been made to computer operating systems that have improved their capabilities in security, process management, and multiprocessor programming.(Ramadhani and Matto, 2015).This review article attempts to examine contemporary operating systems in terms of security, memory management, and some issues related to various operating systems.

For computer security, social and technical issues are always emerging. Due to system diversity, standards, architecture, methodologies, operating system versions, system hardware, and system requirements, technical problems arise that make it difficult to implement security precautions and norms and difficult to respond to unforeseen issues with risk mitigation circuits and draft director of computer plans. (Coelho, 2021). It is a societal issue that nontechnical users of these technologies are unable to identify needs or safety concerns. Because they feel secure having antivirus software and a firewall sending graphic alerts throughout GUI (Graphical User Interface), to the computer technicians who implement secure measures and support them in the day-to-day challenges in organizations, they do not contribute with higher attention to detail (Cvetkovski, 2021). Additionally, applications are regularly created to take advantage of and misleading users or system administrators. As a result, reputable businesses regularly create and release applications to the market that help users avoid mechanisms that insist on violating computer privacy, such as the sharing of resources like random access memory (Awan *et al.*, 2017).

2. The Problem

For software developers, contemporary operating systems like Android, iOS, and Windows offer a new programming abstraction. The application's user interface is divided into several screens, each of which handles a different task, as opposed to putting all functionality into a single window with numerous dialog boxes. The user moves through a number of screens to do a task. These screens could be from the same program or another. For instance, Android apps use intents directed to action strings to assist the OS in determining which app is the best fit for a given activity. Similar to this, Windows offers "share charms" to assist users in finishing activities with various programs. Finally, iOS uses URL protocol handlers to provide limited application-to-application communication and navigation.

3. Security

Operating system security describes procedures and controls that can guarantee the privacy, availability, and integrity of operating systems. The purpose of OS security is to defend the OS against a variety of dangers, such as misconfigurations, remote intrusions, and malicious software like worms, trojan horses, and other viruses (Swift, 2005). The adoption of control strategies that can shield your assets against unwanted addition, deletion, and theft is often part of OS security. The most popular techniques for securing operating systems include the use of antivirus software and other endpoint security technologies, frequent OS patch updates, a firewall for monitoring network traffic, and enforcement of secure access through least privileges and user restrictions (Bellovin and Smith, 2002).

4. Memory Management

Blocks are allocating chunks of memory that are assigned to various operating applications in order to maximize the system's overall performance. This process is known as memory management. This method aids in keeping track of every memory location, regardless of whether it is free or assigned to a specific process. This method determines which process will receive memory when (Carolina and Carolina, 2013). It also keeps track of how much RAM each process has access to. Since it maintains track of everything, anytime memory is freed or unallocated, the status is updated appropriately.

5. Windows Operating System

Windows operating system is a new generation, liable operating system in super computer with a lot of capabilities. The capabilities in the windows operating system make it more suitable than a mainframe computer in the old days in terms of speed, memory management, and hardware sophistication (Fox, 2020). Windows operating system is an open-source operating system that is reliable to use and it is user friendly, introduced in 1985 by Microsoft Inc. it is

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

considered as a robust software and has more than 90% shares. Windows operating system was created as a graphical user interface over the old MS DOS operating system which is a command line (Adekotujo *et al.*, 2020).

These modern operating systems' ability to multitask, yet still being designed to handle a single interacting user, is one of its most notable features. The requirement for multitasking on personal computers, workstations, and servers is the result of two key advances. First off, applications have grown more intricate and interconnected as a result of microprocessors' increased speed and memory capacity as well as their support for virtual memory. To create a document, for instance, a user could want to utilize a word processor, a drawing software, and a spreadsheet application all at once (Fox, 2020). In figure 1 below, Windows operating system architecture is a layered design consisting of components such as the Windows kernel, user mode components, device drivers, and applications. The Windows kernel provides the foundation for the other components to interact with the hardware and provides memory management, process control, and other core functions. User mode components include the user interface, the graphical subsystem, and the Windows API. Device drivers provide a communication interface between the hardware and the operating system, allowing applications to access the hardware. Applications are programs that run on top of the Windows operating system and provide the user with a way to interact with the system.

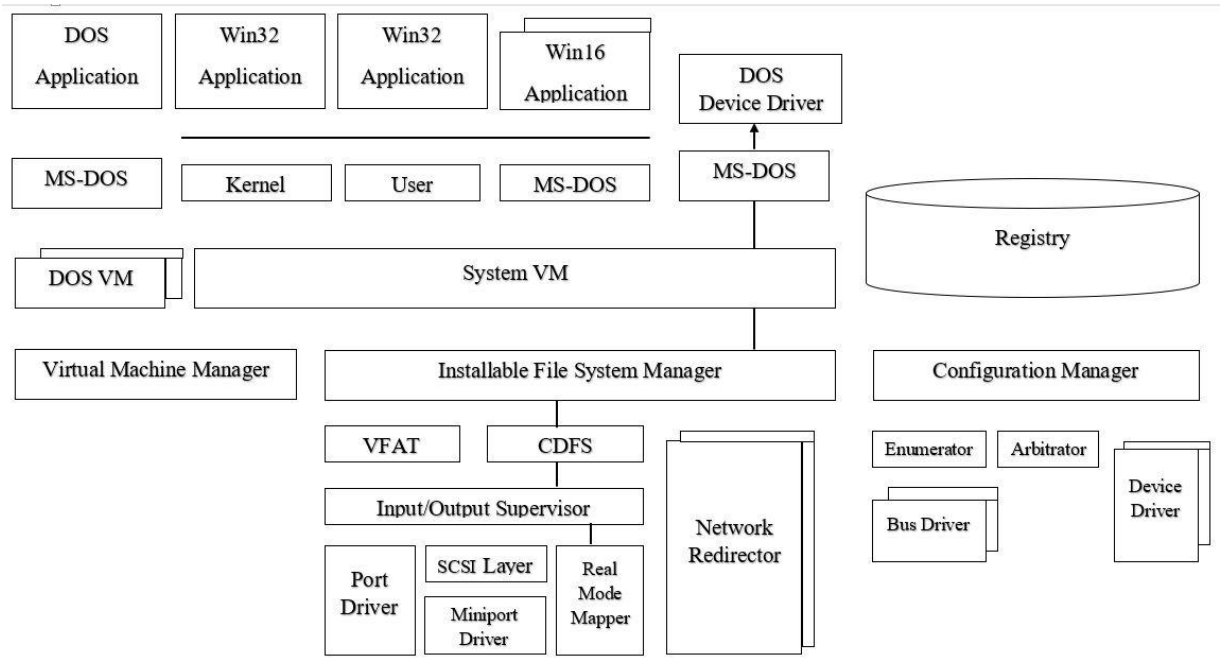

Figure 1: Architecture of Windows Operating System

5.1 Security in Windows Operating System

Windows operating system for all versions have the following vulnerabilities: DOS, SQL injection, overflow, memory corruption, remote code execution etc. in 2010 it was reported that there were about 97 vulnerabilities in windows XP, later the following year 2011 it was 81 vulnerabilities. To detect windows operating system vulnerability, the following vulnerabilities were considered: registry, clipboard, autoplay, and PNG in terms of integrity impact, confidentiality impact, availability, and gained access (Sharma, Kumar and Sharma, 2011).

Table 1: Vulnerability Impact on Windows Operating System

Vulnerability	*Integrity Impact*	*Confidentiality Impact*	*Availability*	*Gained Access*
Registry	Present	Present	Present	Present
Autoplay	Present	Present	Present	Present
Clipboard	Present	Not Present	Present	Present

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

PNG	Not Present	Present	Not Present	Not Present

5.2 Memory Management in Windows Operating System

The allocation of memory and paging operations are managed by the Windows virtual memory manager. The memory manager uses page sizes ranging from 4 Kbytes to 64 Kbytes and is made to work on a range of platforms. The page size for Intel and AMD64 platforms is 4096 bytes, whereas the page size for Intel Itanium processors is 8192 bytes. Each Windows user process on 32-bit platforms sees its own 32-bit address space, giving it access to 4 Gbytes of virtual memory. Each user has 2 Gbytes of available virtual address space, and all processes share the same 2 Gbytes of system space because a portion of this memory is by default set aside for the operating system. There is a setting that increases user space to 3 Gbytes while keeping system space at 1 Gbyte. Using the bigger address space can significantly increase performance for applications like decision support or data mining. This functionality is designed to enable large memory-intensive applications on servers with multiple gigabytes of RAM (Fox, 2020).

6. iOS Operating System

Widely used mobile device Apple's iOS, often known as the iPhone and iPad operating systems, changed with the release of the iPad. iOS uses gestures as a touch interface to control the device. Users can download programs via the Apple Store, which is the repository for iOS applications. Even new users won't have any trouble using the latest iOS version because of how great it looks (Sahani, 2017).

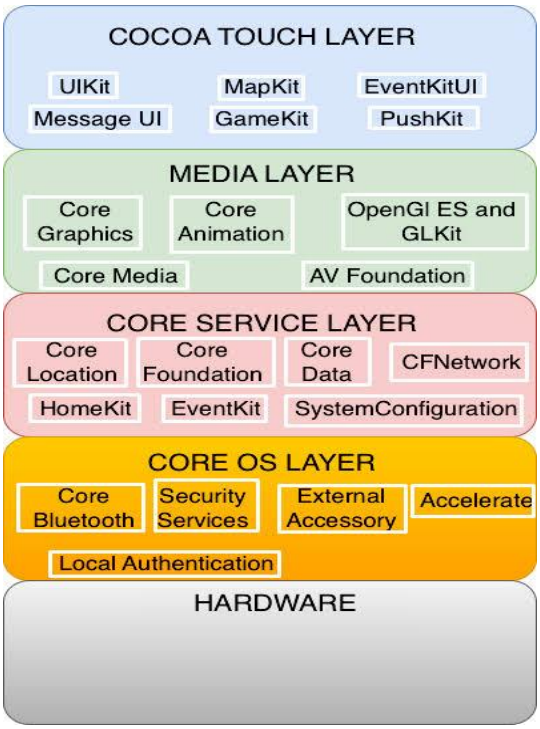

Figure 2: Architecture of iOS Operating System

In figure 2 above, the iOS operating system architecture is a layered structure consisting of four abstraction layers: the Core OS layer, the Core Services layer, the Media layer, and the Cocoa Touch layer. The Core OS layer provides the fundamental system services, such as memory management, power management, and file system access. The Core Services layer provides higher-level services, such as network access, address book access, and so on. The Media layer provides audio, video, and graphics processing capabilities. Finally, the Cocoa Touch layer provides user interface and application frameworks for iOS applications.

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

6.1 Security in iOS Operating System

The limitation of having malware or bloatware was overcome in iOS which allows the device effectively runs faster and beautifully. Unlike android, iOS was developed for only apple devices to provide an optimized service. iOS has an app Find My iPhone which allows the user to locate their device on any device or computer, and the information stored is secured. There is an advanced security feature in iOS which protects the device from threat and these security features are configured by default, these security features include: Data encryption and Touch ID, and the user cannot disable them, they are enable automatically (Sahani, 2017).

6.2 Memory Management in iOS Operating System

Initially, memory management in iOS was non-automatic reference counting. Therefore, there is a need to retain and release the application. But nowadays, it was overcome and it is automatic reference counting, there is no need to retain and release the application. The following issues were encountered during memory management in iOS: free and overwrite user data is still in use; which causes memory corruption and may result in the application's crashing or user data corruption. Not free user data is not in use may causes memory leaking (Lazareska, 2017).

7. Android Operating System

Android is a system software that enables communication between a mobile device, applications, and the user, android mobile operating system was initially Linux kernel which was later modified after being purchased by Google Inc., it was developed and released by members of the open handset alliance and Google. Android is the world's leading mobile operating system ever sold. It has billions of developers for maximizing the device performance (Android and Source, 2008). There is a need for more mobile operating systems due to the higher number of smartphones around the world for convenient use, many users store their data which shows a need for secure mobile operating system. The major used mobile operating system vendors are android and iOS, android is free to use but is more frequent to attack while iOS is secured but complicated. In addition, the security measures in both android and iOS is not enough to secure the data of the user (Sahani, 2017).

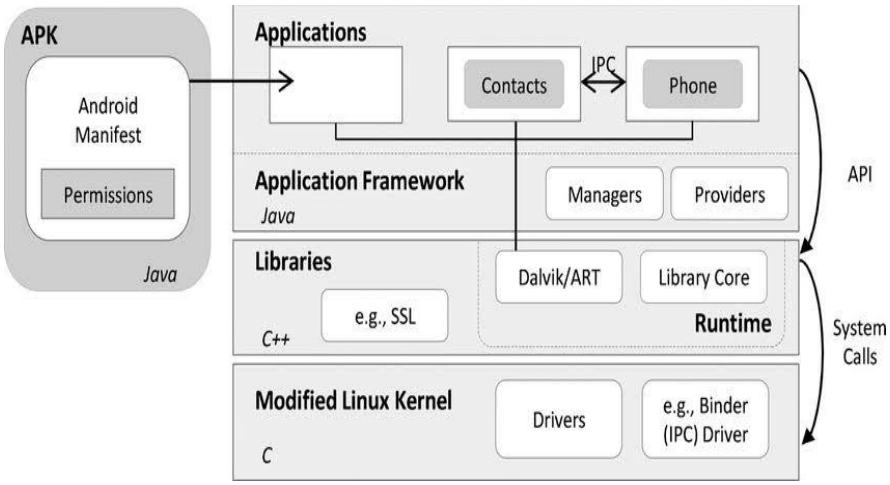

Figure 3: Architecture of Android Operating System

In figure 3 above, the Android operating system architecture is a layered architecture composed of four basic layers: (1) the Linux kernel, (2) the Android Runtime, (3) the Application Framework, and (4) the Applications layer. The Linux kernel provides the operating system's services, such as memory management, process management, and security. The Android Runtime layer sits on top of the Linux kernel and provides a runtime environment for the applications running on the device. The Application Framework layer provides a rich set of libraries and services that developers can use to build applications. The Applications layer is the collection of applications that are available to the user. These applications can include pre-installed applications, as well as applications that are downloaded from the Android Market.

Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

7.1 Security in Android Operating System

Upon using android operating system, user data should be protected, the applications they are using, the device and the network. Android ensure all these components are protected by using security feature like: Linux kernel to ensure security at operating system level, sandbox application, inter-process communication is secured, signing of application, permission grant access and application defined (Singh, 2014). Permission in android operating system is broadly divided into normal permission and dangerous permission, normal permission includes the area where system resources where needed and the permission was granted to the application sandbox, dangerous permission deals with granting permission to use system data by the application which private users data and this can affect the data store in the system (Sahani, 2017).

7.2 Memory Management in Android Operating System

In mobile phones, memory management is a crucial issue, because every user wants his applications to successful run smoothly without any issue. This is now responsible of mobile operating system developers to overcome this limitation in android operating system. Many research has been carried out and implement new techniques in avoiding the limitation of memory management in android operating system. Some system applications are running all the time in mobile phone and they should forever be in memory. In addition, when user is no longer in use of those applications, should either terminate their execution or brought out of the memory so that other application can make use of the memory (Awan *et al.*, 2017).

8. Comparative Analysis of Windows, iOS, and Android

A. Windows

Windows operating system offers a robust memory management system which allows users to optimize their system memory and gain better performance. Windows allows users to adjust the amount of physical RAM, virtual memory, page file size, and maximum memory size, as well as to manage the memory usage of individual applications. This helps users to run tasks more efficiently, and can even help to prevent system crashes.

Windows also offers a powerful security system that helps to protect the system and its files from malicious attacks. It includes features such as Windows Defender, Windows Firewall, Windows Update, and BitLocker. Windows Defender provides a comprehensive anti-virus and anti-spyware solution that can protect against many threats. Windows Firewall helps to protect the system from external threats, while Windows Update helps to keep the system up to date with the latest security patches. BitLocker helps to encrypt data on the system, providing an additional layer of security.

B. iOS

iOS offers a powerful and efficient memory management system, which makes it easier to manage your data and applications. It uses a number of techniques such as virtual memory, memory mapping, and memory compaction to optimize memory usage. Additionally, iOS offers a unified memory architecture, which makes it easier to access multiple programs simultaneously. This helps to ensure that applications can run smoothly and use less memory.

iOS also offers a strong security system. All iOS devices are equipped with hardware encryption and data protection, which helps to protect user data from being accessed without permission. Additionally, iOS offers a secure boot feature, which prevents malicious code from being loaded onto the device. Furthermore, all Apple devices are equipped with Touch ID and Face ID, which adds an additional layer of security to protect user data.

C. Android

Android provides a powerful and efficient memory management system. It uses garbage collection and a virtual machine to manage memory in an organized and efficient way. The Android runtime (ART) uses a “mark-and-sweep” garbage collector, which helps reclaim memory quickly and efficiently. Android also uses a virtual machine to ensure that applications run in a sandbox environment and can’t access other applications or system resources without permission.

Android is designed to be secure from the start. The operating system is regularly updated with the latest security patches, and it has features like app permission control and encryption that helps keep users’ data secure. Android also

SLUJST
Sule Lamido University Journal of Science & Technology Vol. 6 No. 1&2 [March, 2023], pp. 131-138
https://doi.org/10.56471/slujst.v6i.353
Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

has a built-in malware scanner that scans for malicious software and apps and automatically removes them. Google Play Protect also scans installed apps for any malicious behavior. Additionally, Android devices come with a secure boot process that helps protect against malicious attacks and malicious software.

8.1 Quality Comparison between Windows, Android, and iOS

	Windows	**Android**	**iOS**
Manufacturer	Microsoft Inc.	Open-source OS designed &developed by Android Inc. Google is now the current owner	Apple Inc. closed, with components that are source openly
Development and Distribution	Developed and distributed by Microsoft Computer	OHA (Open Handset Alliance)	Apple Inc. developed and distributed iOS
Computer Architecture Supported	x86, x86-64 Target	Android-x86 powered by AMD and Intelx86 processors.	ARM Smartphone
Target System Type	Workstation, Personal Computer, Media Centre, Tablet PC, Embedded, NTFS,	Consumer, Enterprise, education	Smartphone, music system player, Tablet system/computer
File System Supported	NTFS, FAT & exFAT with ISO 9660; UDF, 3rd Party driver that supports file system ext2, and ext3, ReiserFS, and HFS	Ext4	HFS+, FTP
User Friendly for Lay Users	Very User Friendly	Very User Friendly	Very User Friendly
Integrated Firewall	Windows Firewall	Iptables	Firewall-IP for iOS
Security Threats	Huge	Negligible	Negligible
Shell Terminal	CMD	Mosh	Blink Shell
Kernel Type	Hybrid	Linux Kernel	XNU kernel of Darwin
Reliability	Great	Could be unstable	Greater More than Android
Compatibility	Can coexist on local networks with Windows, BSD, Macs, and other Unix-like systems. More compatible.	Better than iOS	Compatibility is fair

9. Conclusion

Android and Windows operating systems are more widely used than iOS, because of their dependability, usability, accessibility, and compatibility. Compared to iOS and Android operating systems, the Windows operating system is much more susceptible to security threats. Because of this, iOS has more security features than the other operating systems. All operating systems effectively manage device memory according to how their authors intended them to, albeit there may be some differences.

Online ISSN: 2736-0903
Print ISSN: 2736-089X
www.slujst.edu.ng

Abbreviations

The following abbreviation are used in this paper:

OS's	Operating Systems
CPU	Central Processing Unit
URL	Uniform Resource Locator
RAM	Random Access Memory
DoS	Denial of Service
SQL	Structural Query Language

References

Adekotujo, A. *et al.* (2020) 'A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android and iOS', *International Journal of Computer Applications*, 176(39), pp. 16–23. doi: 10.5120/ijca2020920494.

Android, T. and Source, O. (2008) 'Android (operating system)'.

Awan, K. M. *et al.* (2017) 'Resource Management and Security issues in Mobile Phone Operating Systems : A Comparative Analysis', pp. 1–18.

Baumann, A. *et al.* (2007) 'Reboots are for Hardware : Challenges and Solutions to Updating an Operating System on the Fly'.

Bellovin, S. M. and Smith, J. M. (2002) 'Sub-Operating Systems : A New Approach to Application Security', *In Proceedings of the 10th workshop on ACM SIGOPS European workshop*, pp. 108–115.

Carolina, N. and Carolina, N. (2013) 'Preventing Accidental Data Disclosure in Modern Operating Systems', *In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1029–1042.

Coelho, N. M. (2021) 'ScienceDirect ScienceDirect New Methodology for the Development of Secure and / Paranoid Operating Systems Mateus-Coelho * of Secure and Paranoid A New Methodology for Nuno the Development', *Procedia Computer Science*, 181(2019), pp. 1207–1215. doi: 10.1016/j.procs.2021.01.318.

Cvetkovski, A. (2021) 'OPERATING SYSTEM VIRTUALIZATION IN THE EDUCATION OF COMPUTER SCIENCE STUDENTS', pp. 823–828.

Fox, R. (2020) *The Windows Operating System*, *Information Technology*. doi: 10.1201/9781003050971-10.

Hee, Y. H. *et al.* (2021) 'Embedded operating system and industrial applications : a review', 10(3), pp. 1687–1700. doi: 10.11591/eei.v10i3.2526.

Lazareska, L. (2017) 'Analysis of the Advantages and Disadvantages of Android and iOS Systems and Converting Applications from Android to iOS Platform and Vice Versa', *American Journal of Software Engineering and Applications*, 6(5), p. 116. doi: 10.11648/j.ajsea.20170605.11.

Mei, H. and Guo, Y. (2018) 'Operating Systems for Internetware : Challenges and Future Directions', *In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, pp. 1377–1384.

Ramadhani, A. and Matto, G. (2015) 'Factors Affecting Adoption and Use of New Operating Systems by University Students : A Survey Study in Moshi Co-Operative', 4(11), pp. 719–724.

Sahani, A. (2017) 'Android v/s IOS – The Unceasing Battle', *International Journal of Computer Applications*, 180(3), pp. 23–26. doi: 10.5120/ijca2017915990.

Sharma, G., Kumar, A. and Sharma, V. (2011) 'Windows Operating System Vulnerabilities', *International Journal of Computing and Corporate Research*, 1(3). Available at: http://www.ijccr.com.

Singh, R. (2014) 'An Overview of Android Operating System and Its Security Features', *Engineering Research and Applications*, 4(2), pp. 519–521.

Swift, M. M. (2005) 'Improving the Reliability of Commodity Operating Systems'.