Open Access Journal of Computer Science and Engineering
Volume 1, Issue 1, 2024, PP: 51-66
www.aytinpublications.com

Research Article

Securing the Future of Mobility: Understanding the Security Perspectives of Cybersecurity, Operating Systems (OS) Security, Mobile Computing

Zarif Bin Akhtar[1*]

[1]*Department of Computing, Institute of Electrical and Electronics Engineers (IEEE), USA.*

Corresponding Author: Zarif Bin Akhtar, Department of Computing, Institute of Electrical and Electronics Engineers (IEEE), USA.

Abstract

This research investigation explores the security landscape in terms of Operating Systems (OS) security and the two dominant mobile operating systems, Android and Apple iOS, in response to the escalating concerns surrounding data privacy and cybersecurity in the realm of the security ecosystem. Through a multidisciplinary methodology comprising data processing evaluation, technical analysis, vulnerability assessment, comparative analysis, real-world case studies, and expert interviews, the research aims to evaluate the efficacy of the security measures implemented by cybersecurity terminologies within protecting user data and mitigating cyber threats. Commencing with an extensive synthesizes for existing research, industry reports, and scholarly articles to contextualize the current state of mobile operating system security. Simultaneously, the security measures employed by both operating systems, such as encryption algorithms, secure boot mechanisms, app sandboxing, and permission models, are evaluated to gauge their effectiveness in thwarting cyber threats. Through a comparative analysis, the exploration elucidates the divergent security postures of mobile computing Android, iOS, delineating their respective strengths and weaknesses. Noteworthy cybersecurity of OS disparities in security architectures, update mechanisms, ecosystem dynamics are identified, providing insights into their implications for end users, enterprises. The results, findings, offering diverse perspectives on emerging trends, best practices in terms of cybersecurity, OS security, Mobile Technical Computing Security. Ethical considerations remain paramount throughout the research process, ensuring responsible handling of sensitive information. This research contributes valuable insights into OS, Cybersecurity, mobile computing, operating system security, informing policymakers, practitioners, researchers within cybersecurity. By adopting a holistic approach and integrating real-world insights, this research aims to facilitate informed decision-making and foster advancements in terms of security practices.

Keywords: Artificial Intelligence (AI), Cybersecurity, Machine Learning (ML), Mobile Computing, Operating Systems (OS), Privacy, Security.

Article Information

Recieved: 04 November 2024

Accepted: 19 November 2024

Published: 27 November 2024

Cite this article as:

Zarif Bin Akhtar. Securing the Future of Mobility: Understanding the Security Perspectives of Cybersecurity, Operating Systems (OS) Security, Mobile Computing. Open Access Journal of Computer Science and Engineering, 2024; 1(1): 51-66.

Introduction

In the ever-evolving landscape of digital interconnectedness, cybersecurity, operating systems (OS) security, mobile operating systems technical computing stand as the linchpin of the modern communications, collaborations, information exchanges. From smartphones to tablets, these compact yet powerful devices have become indispensable companions in our daily lives, seamlessly integrating into every facet of our personal and professional endeavors. However, as we traverse the boundless expanses of cyberspace, we find ourselves confronted by an increasingly sophisticated array of cyber threats that lurk in the shadows, preying on vulnerabilities inherent in various types of peripheral devices and especially the mobile operating systems. The proliferation of mobile devices powered by operating systems such as Android and Apple iOS have ushered in a new era of connectivity and convenience, but it has also brought to the forefront unprecedented challenges in safeguarding our digital identities and sensitive information. In this digital age, where data is the currency of the realm, ensuring the security and integrity of mobile operating systems is paramount to preserving the trust and confidence of users worldwide.

This investigative exploration embarks on a journey into the heart of OS security vulnerabilities, cybersecurity practices, mobile operating system security, exploring the intricate nuances of Android and Apple iOS platforms to unravel their vulnerabilities and resilience against cyber threats and in terms of privacy security. By delving deep into the architecture, vulnerabilities, and security measures of these operating systems, the main aim is towards the illumination of the path forward in fortifying the digital defenses of security platforms. As we will navigate the complex terrain of operating system security, it becomes evident that a multifaceted approach is required to mitigate the diverse and evolving cyber threats that loom on the horizon. From proactive policies and robust encryption protocols to user education and awareness initiatives, this journey will traverse the intersection of technology, policy, and human behavior to forge a resilient digital frontier that safeguards the integrity and confidentiality of the various types of data within the cybersecurity ecosystem. Let's embark on this odyssey into the realm of operating system security, where the quest for digital resilience and cybersecurity excellence takes center stage. Together, let us navigate the frontiers of cyberspace and chart a course towards for a safer, more secure digital future.

Methods and Experimental Analysis

The methodology for conducting a thorough analysis of the operating system security, particularly focusing on Android and Apple iOS, involves a multifaceted approach designed to explore their architecture, vulnerabilities, and security measures very comprehensively and in a step-by-step approach.

Firstly, embarking on an extensive background research, delving into scholarly articles, research papers, and industry reports related to various operating systems security. This investigation serves as the foundation of the research, providing insights into the current landscape, emerging trends, and critical challenges in this domain. Following that, conducting a technical analysis of both cybersecurity practices, security practices, mobile computing particularly within Android and Apple iOS. This entails a deep dive into their underlying architecture, security features, and vulnerabilities. By examining elements such as kernel design, file system structure, memory management mechanisms, and access control policies, the aim is to identify potential weaknesses and assess their resilience against cyber threats.

Subsequently, proceeding with a vulnerability assessment, systematically testing and analyzing known vulnerabilities, exploits, and attack vectors targeting both operating systems. This includes various types of execution processing in terms of common attack surfaces such as application sandboxing, privilege escalation, code signing mechanisms, and network communication protocols to evaluate their susceptibility to exploitation. In parallel, evaluating the security measures implemented by OS security standards in terms of computing terminologies for Android and Apple iOS to mitigate cyber threats effectively. This involves examining built-in security features such as encryption algorithms, secure boot mechanisms, app sandboxing, permission models, and device management capabilities to determine their robustness and adequacy in safeguarding user data and privacy. Moreover, conducting a wide comparative analysis to juxtapose the security posture of Android and Apple iOS, highlighting their respective strengths and weaknesses. This comparative approach involves identifying key differences in security architectures, threat models, update mechanisms, and ecosystem dynamics to discern the relative security implications for end users and enterprises.

Additionally, the exploration incorporates various real-world case studies and use cases involving security incidents, data breaches, and malware outbreaks on areas of cyber space, security domains, Android and Apple iOS platforms. Analyzing these incidents provides valuable insights into the practical implications of security vulnerabilities and the efficacy of security measures in mitigating cyber threats. Furthermore, expertise interviews with cybersecurity professionals, industry experts, and stakeholders in the

mobile ecosystem were conducted to gather diverse perspectives on mobile operating system security. These interviews offer valuable insights into emerging trends, best practices, and evolving threat landscapes, enriching our analysis with real-world insights and expert opinions. Throughout the research process, ethical considerations remained paramount, ensuring responsible handling of sensitive information and adherence to ethical guidelines in data collection, analysis, and reporting. By employing this comprehensive methodology, the aim was to conduct a rigorous and insightful analysis of operating system security, contributing to a deeper understanding of the evolving threat landscape and best practices in safeguarding user data and privacy in the cybersecurity ecosystem.

Background Research and Available Knowledge

Over the past two decades, the Internet has become an integral part of global communication, significantly impacting various aspects of society and the economy. With innovations and decreasing costs, the Internet now boasts around 3 billion users worldwide, generating billions of dollars annually for the global economy. Cyberspace, encompassing economic, commercial, cultural, social, and governmental activities, has become the primary arena for interactions at all levels. Vital infrastructures and sensitive systems operate within cyberspace, highlighting its critical role in modern society [1-6]. The increasing reliance on cyberspace has elevated its importance in measuring a country's development, with indicators related to cyberspace contributing significantly to the Gross Domestic Product (GDP). Furthermore, citizens' lives are intricately connected to cyberspace, with most media activities, financial transactions, and daily interactions occurring within this realm. As a result, any instability or security challenges in cyberspace directly impact various aspects of citizens' lives, underscoring its significance in contemporary society [7-12]. Despite its numerous benefits, cyberspace presents new security challenges to governments worldwide. Factors such as low entry costs, anonymity, and the uncertainty of the geographical origin of threats have empowered both strong and weak actors, including governments, organized groups, terrorist organizations, and individuals, to engage in malicious activities. This has given rise to cyber threats such as cyber warfare, cybercrime, cyber terrorism, and cyber espionage, which pose significant challenges to traditional notions of national security [13,14]. Unlike traditional national security threats, cyber threats are often non-transparent and perpetrated by actors who are difficult to identify geographically. This presents a challenge to traditional national security measures, which may be ineffective in addressing threats in cyberspace. Analysts have long speculated about the potential consequences of cyber-attacks, including severe physical or economic damage resulting from disruptions to financial systems, stock markets, power plants, and air traffic control systems [15,16]. The lack of a clear and comprehensive definition of a cyber-attack complicates efforts to address these complex threats and provide legal analysis and advice. A universally accepted definition of a cyber-attack is essential for establishing a legal framework to identify and address the consequences of such attacks. Without a clear definition, legal interpretations and practices may vary, leading to contradictory legal conclusions. Therefore, there is a pressing need for an acceptable definition of a cyber-attack to guide legal discourse and analysis. This research aims to explore the nature of cyber-attacks, classify them, and examine existing definitions from the perspective of international experts and organizations. By analyzing the various characteristics of cyber-attacks and analyzing existing definitions, this research seeks to contribute to the understanding and legal framework surrounding cyber threats in contemporary society. The focus of cybercriminal activity has increasingly shifted towards the operating systems Android and Apple iOS, given the widespread usage of mobile devices and their unique vulnerabilities.

Therefore, conducting a comparative study of these operating systems is crucial to understanding their vulnerabilities and developing effective methods, policies, and security systems to protect data. Mobile phones, being small embedded devices, possess distinctive characteristics that make them susceptible to cyber threats. They facilitate various activities such as text messaging, multimedia sharing, and collaborative work through social networks, which significantly increases the exchange and handling of confidential information. However, this also exposes them to cybersecurity failures and the risk of data loss or theft due to the escalating cybercrime targeting mobile devices [17,18,19]. Research in the field of information security has highlighted the growing concern regarding information theft, driven by the lack of security education among a large number of users and the widespread use of mobile devices. Both Android and iOS operating systems have become prime targets for attackers due to their prevalence and accessibility. Understanding the security landscape of these operating systems is paramount for society's digital safety. Developing a basic culture of information security, including password management, email security, protection

against malicious software, and privacy protection from digital spies, is crucial in mitigating the risks posed by cyber threats [20,21]. Despite the compatibility of both Android and iOS operating systems, they differ significantly in terms of their susceptibility to viruses and other forms of cyber-attacks. This discrepancy arises from differences in their underlying core (kernel) architecture, which dictates the coding and programming languages used. Viruses are programmed in specific languages, and for an attack to be successful, it must target an operating system coded in the same language. Hence, it is imperative to study Android and iOS separately to understand their unique security vulnerabilities and develop tailored security measures [22-30].

The choice of this research topic stems from the need to determine which operating system, Android or Apple iOS, offers greater security and to propose measures to enhance data protection. Given the prevalent challenges associated with safeguarding information, particularly in the digital age, this research aims to contribute towards improving cybersecurity practices and fortifying the security posture of operating systems. By identifying vulnerabilities and proposing effective security measures, this exploration endeavors to address the current pressing need for enhanced information protection in the realm of mobile computing devices.

Understanding Cyber-Attacks within the Context of Information Operations

Cyber-attacks are a critical component of information operations, which encompass a range of capabilities including electronic warfare, psychological operations, computer network operations, military deception, and security operations. These operations are intricately integrated to penetrate, disrupt, destroy, or manipulate human decision-making processes within national institutions.

Anatomy of Cyber-Attacks

A cyber-attack involves various components within computer network operations, including attack, defense, and exploitation enabling. Unlike traditional network attacks and defense mechanisms, exploitation enabling operations focus primarily on collecting and analyzing information rather than disrupting networks. Such operations may serve as precursors to more overt attacks and can be utilized for purposes such as disseminating information, propaganda, or stealing sensitive computer data.

Tools and Techniques

Tools such as Trap Doors and Sniffers play significant roles in cyber espionage. Trap Doors allow unauthorized external access to software without the user's knowledge, while Sniffers are utilized for the illicit acquisition of usernames and passwords.

Consequences of Cyber Warfare

The ramifications of cyber warfare are vast, ranging from the overthrow of government systems and catastrophic threats to national security to extensive human casualties, internal chaos, and damage to the national economy and cyber assets. Cyber warfare can also lead to disruptions in political and economic relations, erode public confidence, and impact international perceptions of a country.

Scenarios and Definitions

Five distinct scenarios for cyber warfare are outlined, each with varying objectives ranging from government-sponsored cyber espionage to cyber-attacks aimed at facilitating physical aggression or achieving widespread destruction or disruption.

Encryption and Security

Encryption emerges as a crucial tool for protecting sensitive information from cyber threats. However, as computing power advances and encryption methods become more robust, ongoing efforts are required to bolster cryptographic algorithms and mitigate potential vulnerabilities.

Distinguishing Cyber-Attacks

The visualizations with illustrative representations distinguishes between cyber-crime, cyber-warfare, and cyber-attacks. Cyber-crime involves actions by non-governmental entities violating criminal law, while cyber-attacks and cyber-warfare entail deliberate disruptions or destruction of computer networks for political or security objectives. Cyber warfare represents the highest level of cyber-attack, characterized by its severity and potential consequences.

Definitions and Critiques

Various definitions of cyber-attacks provided by specialists are presented and critiqued for their inclusivity and comprehensiveness. These definitions range from actions by countries to disrupt or destroy computer networks to offensive or defensive operations causing injury, death, or property damage. The table 1 and table 2 with figure 1 delves into the intricate landscape of cyber-attacks within the broader context of information operations, highlighting their components, consequences, scenarios, tools, and various definitions from specialists. It underscores the multifaceted nature of cyber warfare and its implications in contemporary conflict and security paradigms.

Table 1. *The main fundamental definitions and the associated concepts of cyberspace*

Title	Definition
Cyber space	Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval and exploitation of information.
Cyber capital	A vital (or sensitive) infrastructure of a country, a vital cyber system, a key information, or individuals belonging to a country.
Cyber vulnerability	Vulnerability refers to a weakness within an asset, security procedures or internal controls, or the implementation of that national cyber asset that can be exploited or activated by internal or external threats to conduct cyber warfare.
Cyber threats	Any event with the ability to strike a blow to missions, tasks, images, national cyber assets or personnel through an information system, through unauthorized access, destruction, disclosure, alteration of information and/or obstruction of (disruptive) service delivery.
Cyber threat level	Cyber threats are able to affect national cyber assets at the transnational, national, institutional, provincial, critical, and critical levels of infrastructure.
Probability of cyber threats	Very high (imminent), high (probable), low (unlikely) and very low (very unlikely)
Intensity of cyber threat	Very high (disaster), high (crisis), moderate (major security incident), low (security incident) and very low (security incident)
Cyber attack	Any unauthorized cyber act aimed at violating the security policy of a cyber-asset and causing damage, disruption or disruption of the services or access to the information of the said national cyber asset is called cyber-attack. Intentional use of a cyber-weapon against an information system in a manner that causes a cyber-incident is also considered cyber-attack.
Cyber weapon	A cyber weapon is a system designed and manufactured to damage the structure or operation of other cyber systems. These systems include bot networks, logic bombs, cyber vulnerability exploitation software, malware, and traffic generation systems to prevent service attacks and distributed service.
Cyber warfare	Cyber warfare is the highest level and most complex type of cyber-attack (cyber operation) that is carried out against the national cyber interests of countries and will have the most severe consequences.
Cyber warfare origin	The cyber force of the aggressor country or groups organized under the aggressor states, cyber weapons controlled or abandoned by these forces
Cyber defense	Utilization of all unarmed cyber and non-cyber facilities of a country, to create deterrence, prevention, prevention, timely detection, effective and deterrent response to any cyber attack
Cyber biome	Cyber biome refers to the formation of a native and dynamic cyber environment that is supportive for a country in various fields.
Virus	A virus is a self-replicating program that spreads to other documents and other programs by duplicating itself, and may cause programs to malfunction. A computer virus acts like a biological virus that spreads through its reproduction to cells in the host body. Some of the popular viruses are: NIMDA, SLAMMER, and SASSER.
Hacker	A person who enters a system without permission or who increases his/her access to information to browse, copy, replace, delete or destroy it.

Table 2. *The various distinctions between cyber-crime, cyber-attacks, cyber-warfare*

Type of cyber action	Nature and characteristics
Cyber-crime	Cyber actions taken only by non-governmental attackers.
Cyber-crime	The cyber action is carried out by a computer system and is merely in violation of criminal law.
Cyber-attack and cyber-warfare	The purpose of a cyber-attack is to destroy and disrupt the operation of a computer network.
Cyber-attack and cyber-warfare	The attack must have political or security purposes.
cyber-warfare	The effects of a cyber-attack are the same as an armed attack or the cyber act took place in the context of an armed attack.

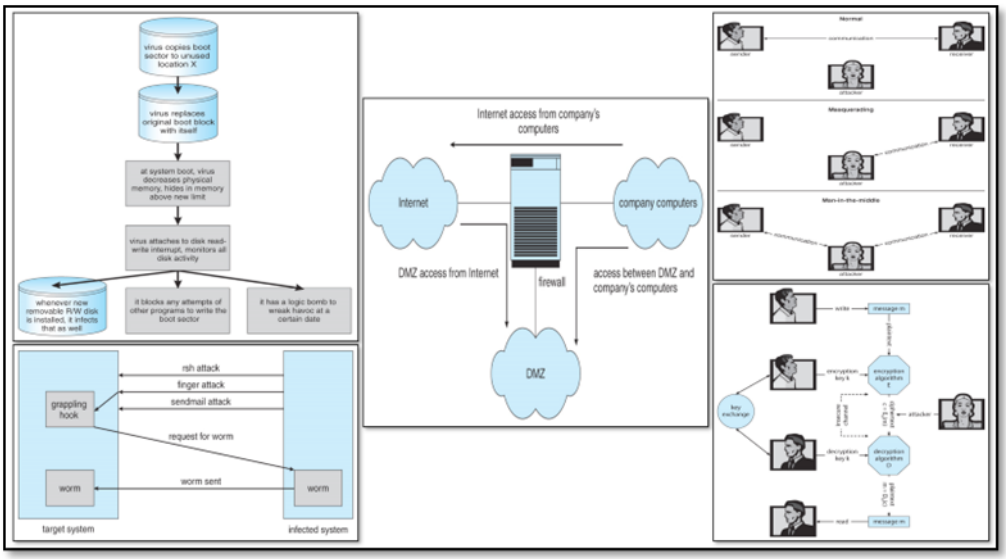

Figure 1. *An overview of Cyber-Threats-Attacks-Security*

Dynamics of Cyber Threats and Security Measures

The global cyberspace presents a complex landscape where national actors with diverse legal, cultural, and strategic interests overlap. The increasing dependence of countries worldwide on cyberspace for communication and control of physical systems renders it inseparable from contemporary security considerations. This analysis explores the multifaceted nature of cyber threats and the evolving security measures within this dynamic environment. Many countries face significant challenges in securing their cyber domains due to the global production of software and hardware, which makes it impossible to guarantee the integrity of supply chains. The scalability of cyberspace distinguishes it from traditional physical threats, as cyber-attacks can have far-reaching effects beyond physical limitations. Additionally, the distributed nature of the cyber domain, controlled by a relatively small number of individuals, presents challenges in achieving comprehensive control.

Cyber threats originate from various sources, including foreign intelligence services engaged in espionage activities, financially motivated groups targeting information infrastructures, and individuals or groups seeking to express political motives through cyber-attacks (hacktivism). Internal dissatisfied agents within organizations also pose significant threats, leveraging their system knowledge for illicit access or data theft.

Furthermore, terrorist groups aim to disrupt vital infrastructure to undermine national security and economy while instilling fear among the populace. A variety of methods are employed in cyber-attacks, including Denial of Service (DoS), logical bombs, abuse tools, sniffers, Trojan horses, viruses, worms, spamming, and botnets. Each method targets different vulnerabilities in computer systems and networks, ranging from disrupting authorized access to embedding destructive code within programs or files.

Research efforts focus on enhancing cyber-security measures to mitigate the impact of cyber-attacks. Studies have explored the impact of cyber security on specific systems, such as the use of Convolutional Neural Networks (CNN) for processing spoofing data in Wide-Area Measurement Systems (WAMS). Other research examines unified cyber-attack response processes, security state approximation methods, decision support systems for optimal security portfolios, and variables affecting cyber-attack possibilities in Nuclear Power Plants (NPPs). Additionally, research highlights the economic implications of cyber-attacks on firms' reputations, financial markets, and long-term performance. The dynamic nature of cyberspace presents complex challenges for national security, with diverse threats originating from various sources and targeting different vulnerabilities. Efforts to enhance cyber-security measures through research and defense strategies are crucial in mitigating the impact of cyber-attacks and safeguarding critical infrastructure and information assets. Understanding the evolving nature of cyber threats and implementing effective defense mechanisms are essential in maintaining the integrity and security of cyberspace.

Cyber Security Policies and Strategies

Cyber security is paramount for the infrastructure of every company and organization, as it safeguards private and customer data against various threats. This section delves into the importance of cyber security measures and explores different types of cyber security, cybercrime methods, and the principles guiding cyber security policies.

Importance of Cyber Security

Organizations that prioritize cyber security can attain high status and achieve success by effectively protecting sensitive information from competitors and abusive entities. Cyber security encompasses practical measures to safeguard information, networks, and data against internal and external threats, ensuring that only authorized individuals have access.

Types of Cyber Security

Network Security: Protects computer networks from disruptors like malware or hacking, employing solutions to keep networks out of reach from unauthorized access.

Application Security: Utilizes hardware and software (e.g., anti-virus programs, encryption) to defend systems against external threats during application development.

Information Security: Safeguards physical and digital data from unauthorized access, disclosure, misuse, and deletion.

Operational Security: Involves processes and decisions to control and protect data, such as user permissions and information storage/sharing protocols.

Cloud Security: Ensures information security in the cloud and monitors on-site attack risks.

User Training: Educates users on cyber security practices to mitigate unpredictable threats, such as avoiding suspicious email attachments and refraining from connecting to anonymous USBs.

Cybercrime Methods

Cybercriminals engage in unauthorized activities involving systems, equipment, or networks, including denial of service attacks, man-in-the-middle attacks, malware infections, and phishing scams.

Principles of Cyber Security Policies: The principles of confidentiality, integrity, and availability (CIA) serve as the foundation of cyber security policies. Confidentiality ensures only authorized access, integrity protects against unauthorized modifications, and availability ensures data and systems are accessible based on service level agreements.

Cyber Security Policy Implementation: The implementation of cyber security policies varies between national and corporate levels, with different departments expected to comply with regulations. Cyber security policies guide organizational practices and decision-making, balancing security measures with operational efficiency.

An Investigative Analysis of Computer viruses within the cellular mobile terminology landscape

In today's interconnected society, the proliferation of viruses and malware presents a significant challenge, leading to numerous economic and financial losses. Understanding these threats is crucial for mitigating potential damages. This research focuses on studying the Android and Apple iOS operating systems, which are primary targets for information theft via spyware. Spyware, a type of malware, clandestinely transmits sensitive information to remote computers, often targeting banking credentials, posing a significant threat to user privacy and financial security. Quissanga defines computer viruses in mobile phones as malicious software programmed to infect the operating system, disrupt normal software functioning, and replicate throughout the system. Despite their destructive potential, phone viruses remain relatively obscure, with varying degrees of destructiveness aimed at covertly obtaining confidential user information. Recognizing the techniques employed by cybercriminals is imperative, highlighting the importance of vigilance and robust security measures. The behavior of cybercriminals, as exemplified by the Talk Talk cyber-attack, underscores the far-reaching consequences of data breaches. Such attacks result in substantial financial losses, erosion of customer trust, and potential identity fraud, highlighting the urgent need for enhanced cybersecurity measures. Differentiating between the security of Android and Apple iOS operating systems is a key focus of this research, given their widespread use across various demographics. Understanding their vulnerabilities is crucial for developing effective security mechanisms at both the organizational and individual levels. It is essential to recognize information security as a global concern with far-reaching implications, ranging from diplomatic tensions to corporate bankruptcies, stemming from security failures. Despite previous studies lacking conclusive evidence on a universal security protocol for these operating systems, preventive measures are paramount. Cybercriminals constantly exploit vulnerabilities in newly launched systems, emphasizing the need for proactive security measures. The transmission of viruses via various channels, such as email, social networks, and infected media, underscores the multifaceted nature of the threat landscape. Viruses in mobile phones pose unique challenges due to the diversity of operating systems and their respective internal structures. While users play a role in safeguarding their devices, some companies fall short in adequately protecting customer information, necessitating collective efforts to enhance cybersecurity resilience. Proposed viruses targeting mobile

phone operating systems underscore the evolving nature of malware threats, requiring continuous classification and analysis to identify emerging trends and patterns.

Despite the rapid growth of malware, many users lack basic awareness of potential risks, highlighting the importance of ongoing research and education initiatives in cybersecurity. To provide an idea table 3 sheds some insights on the matter of perspective.

Table 3. Computer Viruses Within The Cellular Mobile Terminology

No.	Virus/worm name/year (updated)	Operating system
1.	Cabir A (June 2004)	Symbian
2.	Caballo de Troya (March 2017)	Symbian, Windows, Android and Mac OS X
3.	CommWarrior (October 2018)	Symbian and Android
4.	Crossover (March 2011)	Windows Mobile
5.	Doomboot (July 2019)	Symbian
6.	Liberty (September 2007)	Palm OS
7.	RedBrowser (September 2017)	J2ME
8.	FlexiSpy (June 2019)	Symbian and Android
9.	Skuller (June 2004)	Symbian
10.	Gingermaster (April 2011)	Android
11.	Ikee (November 2009)	iPhone OS (IOS)
12.	DroidKungFu (June 2011)	Android
13.	Zitmo (April 2018)	Symbian, Android
14.	YiSpecter (April 2018)	iPhone OS (iOS)

The Security Considerations for Mobile Computing Operating Systems (Android and iOS)

Mobile operating systems, notably Android and Apple iOS, are subject to various vulnerabilities and security threats, necessitating a comprehensive approach to mitigate risks and protect user data.

Android Vulnerabilities

Android, developed by Google, offers a flexible platform due to its open-source nature. However, this openness also renders it susceptible to malware attacks. Based on the Linux kernel, Android shares similarities in functionalities like security and memory management. Yet, its widespread adoption combined with a lack of information security culture among users has made it a prime target for cybercriminals. Instances of malware, including viruses and spyware, underscore the urgent need for robust security policies and measures.

Apple iOS Security Measures

In contrast, Apple's iOS is a closed system with stringent restrictions aimed at preventing malware from infiltrating the system. Despite its security measures, vulnerabilities exist, evidenced by security flaws and the potential for cyber-attacks, particularly on jailbroken devices. The iOS system, renowned for its aesthetics and user experience, also faces security challenges, such as attacks targeting the root password and malicious software infiltrating the App Store.

User Vulnerabilities and Unsafe Practices

Users contribute to security vulnerabilities through unsafe practices, including installing applications from untrusted sources and enabling jailbreak. Engaging in insecure online behaviors, such as opening suspicious emails or making purchases on unsecured websites, exposes users to various cyber risks, including identity theft and financial fraud.

Proposed Security Measures

To mitigate these risks, a range of security measures is proposed, encompassing preventive, detective, and corrective actions. These measures include assigning strong passwords, utilizing cryptographic techniques, enabling firewalls, and implementing virtual private networks (VPNs) for data encryption and privacy protection. The importance of user education and awareness regarding information security practices is emphasized, underlining the collective responsibility of both users and companies in safeguarding mobile devices and data. Addressing security considerations for mobile operating systems requires a multifaceted approach, integrating technical solutions, user education, and collaborative efforts. By implementing robust security measures and promoting user awareness, the risks posed by cyber threats in the mobile ecosystem can be effectively mitigated, ensuring the protection of user information and privacy.

Future Directions Overview within Mobile Computing and Operating Systems (OS) Security

When comparing the Android and Apple iOS operating systems in terms of their susceptibility to computer viruses, it's evident that both have their vulnerabilities despite offering a certain level of safety. While Android's open platform facilitates a larger developer community, it also exposes it to more potential vulnerabilities compared to the closed and meticulously vetted ecosystem of Apple's iOS. The iOS system, built with a different programming language than Android, boasts greater protection due to its stringent app vetting process and restricted installation permissions outside of the App Store.

Prevalence of Cyber Attacks on Mobile Operating Systems

Both Android and iOS are prime targets for cyber-attacks due to their widespread usage, making them attractive targets for malicious actors. Social networks, in particular, have become focal points for cyber contaminations, highlighting the need for enhanced security measures within these platforms.

Advancements in iOS Security

Apple has implemented rigorous measures within the iOS ecosystem to safeguard users from malicious apps, including a meticulous vetting process for apps before they are available on the App Store. Additionally, tools like PiOS have been developed to analyze Objective-C source code and Mach-Obinaries data flowcharts, effectively identifying and mitigating potential information leaks on mobile devices.

User Practices and Company Responsibilities

While users play a crucial role in ensuring the security of their devices, some insecure practices make them susceptible to cyber-attacks, leading to economic losses such as credit card cloning. However, it's not solely the responsibility of users; companies must also prioritize the protection of customer information and provide basic training on information security techniques to their employees.

Essential Security Protocols and Measures

To bolster security, adherence to protocols such as authenticity, confidentiality, integrity, and intimacy is essential. Implementing a combination of preventive, detective, and corrective measures is crucial to mitigate risks effectively. Furthermore, utilizing security applications recommended for mobile systems can further enhance the overall security posture of devices.

While Android and iOS strive to provide secure mobile operating systems, continued vigilance, adherence to best practices, and the adoption of advanced security measures are imperative to combat evolving cyber threats effectively.

Results and Findings

The security problem within operating systems encompasses protecting systems from deliberate attacks, whether internal or external, aimed at stealing information, modifying data, or causing intentional disruption. Breaches of confidentiality involve the theft of private or sensitive data like credit card numbers, trade secrets, or financial information. Breaches of integrity entail unauthorized modifications to data, potentially leading to serious consequences, such as creating security vulnerabilities.

Breaches of availability involve the unauthorized destruction of data or disruption of services, often for malicious intent or bragging rights. Theft of service refers to the unauthorized use of resources, including CPU cycles or network services. Denial of service (DoS) attacks aim to overwhelm systems with excessive requests, preventing legitimate users from accessing services.

Various attack methods, such as masquerading, replay attacks, and social engineering, are employed by attackers to breach system security. Operating systems must be protected at multiple levels: physical, human, operating system, and network. Physical security involves safeguarding hardware and backup tapes to prevent data theft. Human security aims to ensure that authorized users cannot be coerced into breaching security, often targeted through social engineering tactics like phishing or dumpster diving for passwords.

Operating system security involves protecting against various security breaches like denial-of-service attacks, memory-access violations, or unauthorized program launches. Network security is crucial as modern computing heavily relies on network communications, necessitating protection against external attacks and securing local systems from network-based threats. Program threats pose significant risks to modern systems, including Trojan horses, trap doors, logic bombs, stack and buffer overflows, and viruses.

Trojan horses are programs that perform malicious actions while appearing legitimate, often exploiting vulnerabilities like long search paths or login emulators to steal user credentials. Trap doors are deliberate security holes inserted by designers or hackers to gain unauthorized access to systems, while logic bombs execute malicious actions under specific conditions, such as a certain date or

time. Stack and buffer overflows exploit bugs in system code to overwrite memory addresses and execute nefarious code, leading to security breaches.

Viruses are fragments of code embedded in legitimate programs, designed to replicate and cause harm, with various forms like file viruses, boot viruses, macro viruses, and others, each presenting unique challenges for detection and mitigation. Understanding and addressing the diverse threats to operating system security is essential in today's digital landscape.

Robust security measures must be implemented at multiple levels to protect against deliberate attacks, ranging from physical safeguards to network security protocols. By recognizing common program threats like Trojan horses and viruses and implementing preventive measures, organizations can enhance the security posture of their systems and mitigate potential risks associated with cyberattacks.

Additionally, ongoing vigilance, regular updates, and collaboration within the cybersecurity community are crucial for staying ahead of evolving threats and maintaining the integrity, confidentiality, and availability of operating systems and associated data.

In the realm of cybersecurity, system and network threats pose significant risks to the integrity and functionality of operating systems and interconnected networks. These threats manifest in various forms, targeting vulnerabilities within software programs or exploiting weaknesses in network infrastructure. Understanding the nature of these threats is crucial for developing effective defense strategies.

Worms

One prominent threat is worms, malicious processes that autonomously replicate themselves to propagate across systems and networks. These self-replicating entities consume system resources and can cause widespread disruption by overwhelming network infrastructure.

An infamous example is the Morris Internet worm, unleashed in 1988, which swiftly traversed the early Internet by exploiting vulnerabilities in UNIX-based systems. By exploiting weaknesses in utilities like remote shell and sendmail, the Morris worm underscored the importance of addressing software vulnerabilities to prevent large-scale attacks.

Port Scanning

Port scanning, while not inherently malicious, is a reconnaissance technique employed by attackers to identify vulnerable network ports for potential exploitation. Although it serves as a precursor to attacks rather than an attack itself, port scanning can reveal critical security gaps in network defenses. Tools like nmap and nessus empower administrators to conduct proactive vulnerability assessments without causing harm to systems, highlighting the importance of comprehensive security measures.

Denial of Service (DOS)

Denial of Service (DoS) attacks aim to disrupt system or network services by overwhelming them with a flood of requests, rendering them inaccessible to legitimate users. These attacks can exploit vulnerabilities in system configurations or security features, such as account lockout mechanisms, to effectively disrupt services. Notably, DoS attacks can stem from both malicious intent and unintentional causes, emphasizing the need for robust system management practices to mitigate disruptions.

Cryptography as a Security Tool

Encryption: Cryptography plays a pivotal role in securing network communications by encoding messages to ensure confidentiality and integrity. Encryption algorithms, such as DES, AES, and RSA, utilize keys to transform plaintext messages into ciphertext, which can only be deciphered by authorized parties possessing the corresponding decryption keys. Symmetric encryption employs a single key for both encryption and decryption, while asymmetric encryption uses separate keys, offering enhanced security but at a higher computational cost.

Authentication and Key Distribution: Authentication mechanisms verify the identity of message senders, ensuring the integrity and authenticity of transmitted data. Key distribution is a critical aspect of cryptography, addressing the challenge of securely sharing encryption keys between communicating parties. Asymmetric encryption facilitates key distribution by allowing the public dissemination of encryption keys while safeguarding decryption keys, mitigating risks associated with key management.

Implementation of Cryptography: Cryptography is implemented across multiple layers of network protocols, including physical, data link, network, transport, and application layers. Encryption and security measures can be applied at different layers, each with its advantages and considerations. Protocols like IPSec and SSL/TLS exemplify cryptographic implementations at the network and transport layers, respectively, facilitating secure communication channels and Virtual Private Networks (VPNs) over public networks.

User authentication is a fundamental aspect of system security, ensuring that only authorized users can access resources and perform specific tasks. This area needs to be

explored through various methods of user authentication, focusing on passwords, encrypted passwords, one-time passwords, biometrics, and their associated vulnerabilities [27-30]. Passwords are the most common form of user authentication, requiring users to input a secret passphrase to verify their identity. While theoretically, separate passwords could be assigned for different activities, most systems opt for a single password for user identification, followed by authorization based on this identity. However, passwords are vulnerable to various attacks, including intelligent guessing, brute-force attacks, and shoulder surfing. Passwords face numerous vulnerabilities, including susceptibility to guessing and observation, such as shoulder surfing. Moreover, passwords can be intercepted through packet sniffing or compromised through social engineering tactics. Long and complex passwords, while more secure, may be written down or shared, undermining their effectiveness. To enhance password security, modern systems encrypt passwords rather than storing them in plain text. Encrypted passwords are matched against stored encrypted versions during authentication, minimizing the risk of password exposure.

However, encrypted passwords must be stored securely, as compromising the encryption scheme can lead to unauthorized access. One-time passwords offer increased security by generating unique passwords for each authentication attempt. These passwords resist attacks such as interception and replay attacks, as they are valid for a single use only. Methods like challenge-response systems and electronic cards with time-based codes provide additional layers of security. Biometric authentication uses physical characteristics unique to individuals, such as fingerprints or retinal patterns, to verify identity. While biometrics offer strong security, challenges related to usability and physiological changes must be addressed. Technologies like fingerprint scanners, palm readers, and voiceprint analyzers are increasingly employed for biometric authentication. After exploring user authentication methods, this section delves into implementing security defenses to safeguard systems and networks against unauthorized access and attacks. Topics include security policies, vulnerability assessment, intrusion detection, virus protection, auditing, accounting, and logging. A well-defined security policy serves as a foundation for implementing security measures, outlining guidelines for system security, access control, and data protection. A comprehensive security policy is essential for maintaining a secure environment and should be regularly updated to address emerging threats and vulnerabilities. Periodic vulnerability assessments are crucial for identifying and mitigating security weaknesses within systems and networks.

Techniques such as port scanning, password checks, and system file integrity checks are employed to detect vulnerabilities and unauthorized access points. Intrusion detection systems monitor for unauthorized access attempts and security breaches, alerting administrators to potential threats. Signature-based detection and anomaly detection are common approaches to detecting intrusions, each with its advantages and limitations. Effective virus protection measures are essential for detecting and preventing malware infections. Modern antivirus programs utilize signature-based detection and behavior analysis to identify and neutralize viruses, protecting systems from malicious software threats. Auditing, accounting, and logging mechanisms record system activities and access attempts, providing valuable information for detecting and investigating security incidents. Detailed logging helps identify security breaches, track user activities, and analyze system performance.

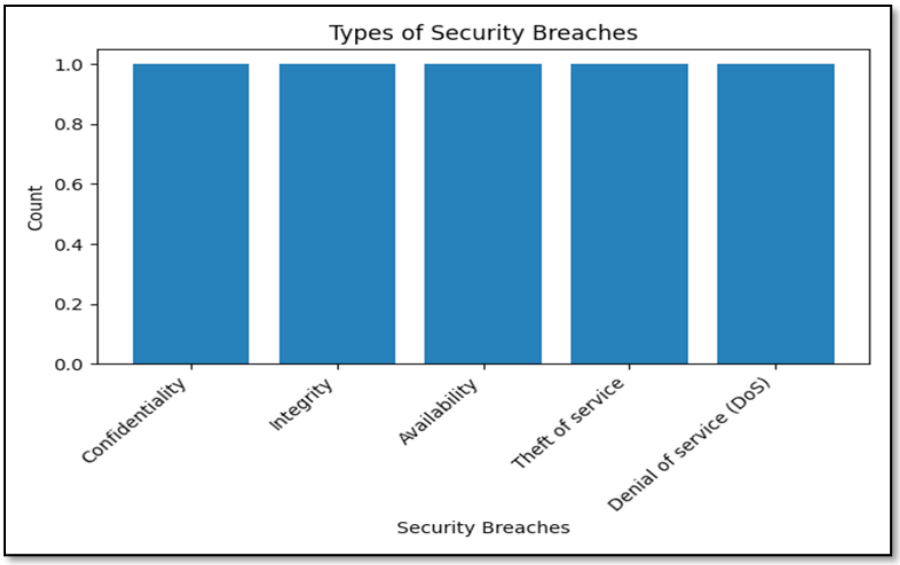

Figure 2. *A visualization overview of the research results and findings 1*

User authentication is a critical component of system security, and implementing robust security defenses is essential for safeguarding systems and networks against evolving threats. By employing secure authentication methods and implementing effective security measures, organizations can enhance their resilience to cybersecurity risks and protect sensitive data from unauthorized access and malicious activities. To better understand the figures 2, 3, 4, 5, 6 illustrations represent the border overview for the perspective of the matter.

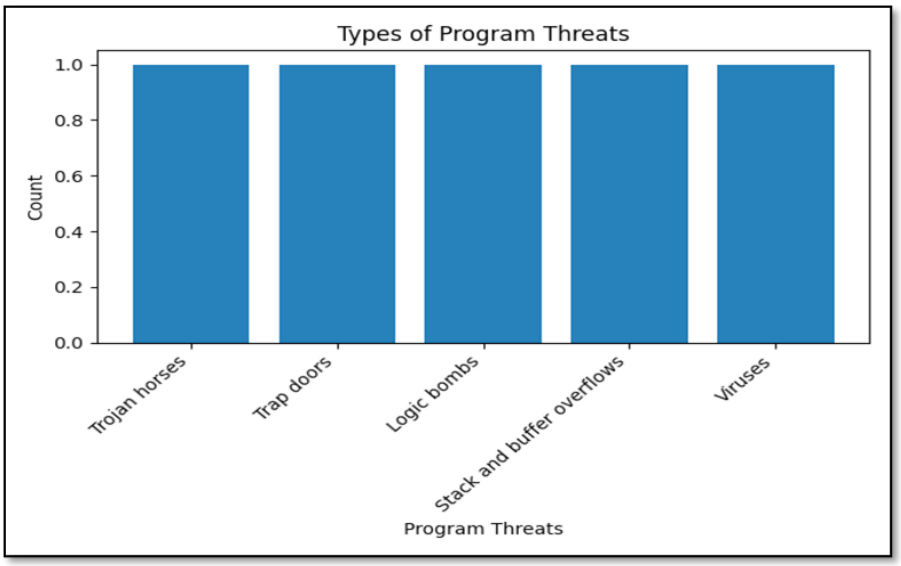

Figure 3. *A visualization overview of the research results and findings 2*

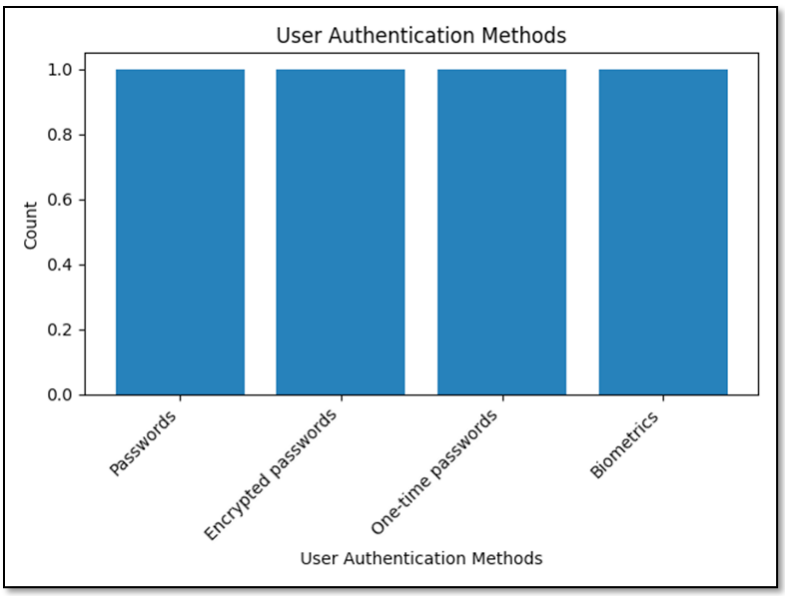

Figure 4. *A visualization overview of the research results and findings 3*

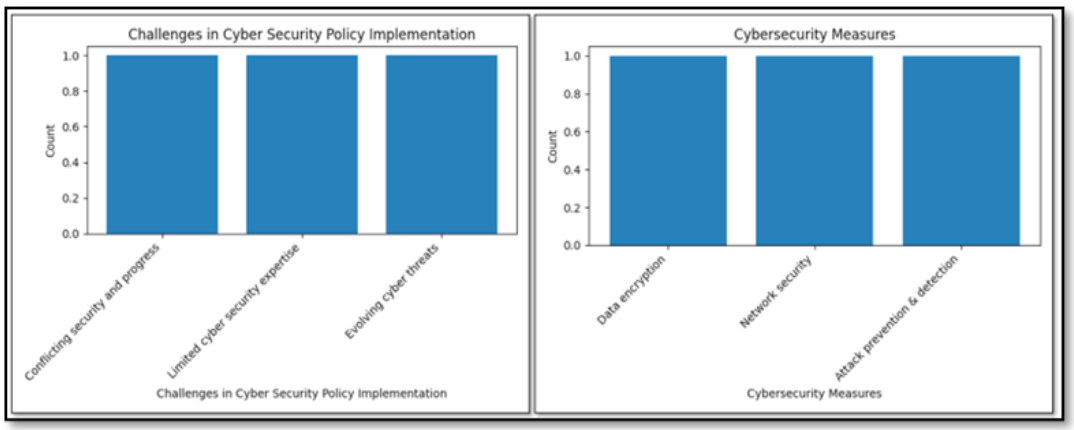

Figure 5. *A visualization overview of the research results and findings 4*

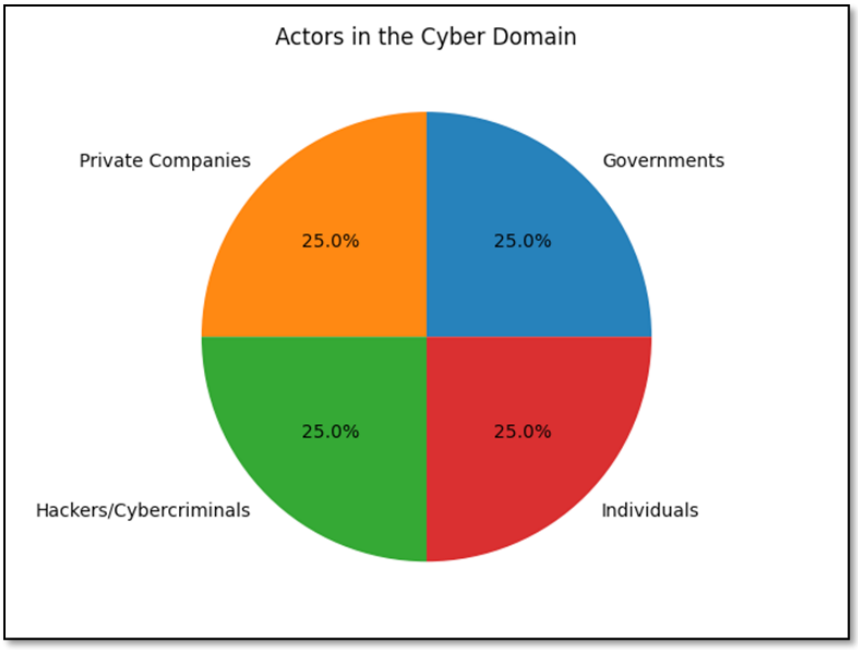

Figure 6. *A visualization overview of the research results and findings 5*

Discussions

Challenges in cyber security policy implementation include the conflict between security measures and technological progress, limited expertise in cyber security, and the evolving landscape of cyber threats. As organizations navigate these challenges, comprehensive cyber security strategies that address all aspects of cyber security are essential for safeguarding against threats and ensuring the integrity of systems and data. In today's digitally-driven landscape, the security of operating systems is of paramount importance to safeguard against a myriad of cyber threats.

Operating systems, the backbone of computer devices, are vulnerable to various forms of attacks such as malware, network intrusions, and hacking attempts, which can lead to data breaches, financial fraud, and service disruptions. Malware, including spyware, adware, bots, and ransomware, poses a significant threat to operating system security by exploiting vulnerabilities to steal data, manipulate system configurations, and disrupt operations. Network attacks like Denial of Service (DoS) and Distributed Denial of Service (DDoS) aim to overwhelm system resources, while hacking attacks target unauthorized access to systems, further compromising security.

To mitigate these threats, cybersecurity plays a pivotal role in defending digital assets against unauthorized access and exploitation by malicious entities. Cybersecurity encompasses a range of measures and technologies including data encryption, network security, and attack prevention and detection. It acts as the primary defense mechanism to safeguard operating systems from cyberattacks, ensuring the security of data and system operations. Robust security measures such as firewalls, intrusion detection systems, and access controls are essential components of cybersecurity, working together to monitor and filter network traffic, detect and block suspicious activities, and enforce user authentication mechanisms.

Furthermore, cybersecurity emphasizes the importance of user awareness and education in maintaining a secure operating system environment. Training programs and awareness campaigns educate users on best practices such as strong password management, safe browsing habits, and identifying and avoiding suspicious emails or attachments. By fostering a culture of security awareness, organizations empower users to actively contribute to operating system protection. Additionally, antivirus software plays a critical role in identifying and removing malicious programs, ensuring the integrity of the operating system and protecting against malware attacks. Regular application of security patches and updates is crucial to addressing newly discovered vulnerabilities and maintaining operating system security. Security patches released by operating system developers address known vulnerabilities and update critical components, safeguarding against potential exploits. Moreover, maintaining secure data backups is essential to recover information in the event of an attack or system crash. Regular data backups stored in secure locations enable users to mitigate the risk of data loss and restore the operating system quickly following a security incident.

Ensuring the security of operating systems requires a comprehensive approach that encompasses robust cybersecurity measures, user education, antivirus software, regular application of security patches, and secure data

backups. By implementing these strategies, organizations and individuals can effectively protect their operating systems from cyber threats and maintain the integrity and security of their data and operations.

Conclusions

In the contemporary era, cyberspace and associated technologies have emerged as crucial sources of power, marking a significant shift in the dynamics of power distribution in the third millennium. The unique characteristics of cyberspace, including its low entry barriers, anonymity, vulnerability, and asymmetry, have led to the phenomenon of power diffusion. While governments have traditionally held sway over power dynamics, the landscape has expanded to include a diverse array of actors such as private companies, organized terrorist and criminal groups, and individuals. Despite the increasing involvement of non-state actors, governments continue to play a pivotal role in shaping this evolving landscape.

This diffusion of power has implications for national security paradigms. The traditional concept of national security, which primarily focused on military threats and safeguarding internal and external borders, has evolved. In the digital age, the risk of threats impacting citizens' quality of life has become a significant concern, blurring the lines between traditional notions of security and broader societal well-being. Moreover, the geographical dimension of cyber threats has become less defined. Unlike traditional military threats with distinct geographical locations, cyber threats transcend borders, making identification and containment more challenging. The vulnerabilities posed by cyber threats are widespread and multidimensional, with the potential for significant damage due to their association with critical networks and infrastructure. Addressing these complex threats requires a departure from traditional approaches reliant solely on military and police force. Governments alone cannot effectively counter cyber threats, necessitating robust cooperation between public and private sectors. Collaboration between governments and the private sector, which share common interests in combating cyber threats, is essential for developing effective strategies and responses. Furthermore, it is crucial to recognize that cyber threats extend beyond governments, posing risks to individuals and companies alike.

The interconnected nature of cyberspace means that no entity is immune to the potential harms posed by cyber threats. In navigating this new landscape of security challenges, traditional theoretical approaches in international relations, which predominantly focus on the role of governments, may fall short. The evolving nature of security in the information age demands a reevaluation of theoretical frameworks to encompass the diverse array of actors and dynamics at play in cyberspace. Failure to adapt theoretical approaches may lead to oversights or confusion in understanding and addressing contemporary security challenges. In terms of the comparative analysis between the Android and iOS mobile operating systems, it becomes evident that iOS offers a higher level of security compared to Android, primarily due to the stringent restrictions and security mechanisms enforced by Apple. While both systems face potential threats from computer viruses, the current concern lies more in other forms of cyber-attacks, particularly spyware designed to clandestinely capture confidential information and transmit it to remote servers, regardless of geographical location.

These spyware attacks represent a significant threat as they enable the comprehensive monitoring of user activities for malicious purposes. Distinctively three primary forms of cyber-attacks have been identified which are online identification of victims, attacks on industrial infrastructure, and targeted attacks on individuals. However, the most pressing issue stems from the negligence of users in practicing proper information security measures. Instances of social engineering, attacks on banking data, credit card cloning, and the installation of software from unauthorized sources outside of official app stores pose significant risks to user data and financial security. To address these concerns and enhance information security, it is imperative to implement robust security policies.

Key recommendations include exercising utmost caution with passwords, utilizing modern WPA encryption for WiFi networks, installing firewall protection even on non-rooted devices, employing tools like Privacy Badger to block unsafe websites, using Panopticlick for web testing, employing VeraCrypt to encrypt important documents, and utilizing encrypted communication applications like Signal for secure phone calls. These measures are essential in mitigating the risks associated with cyber-attacks and protecting user privacy and sensitive information from unauthorized access and exploitation. Operating system security is a critical concern in today's digital landscape, with potential threats posing risks to individuals, organizations, and society as a whole.

Effective implementation of cybersecurity measures is essential to safeguard operating systems against malware, network attacks, and vulnerabilities. By prioritizing cybersecurity, we can ensure the integrity, confidentiality, and availability of operating systems, which are fundamental to modern information technology infrastructure. Proactive measures, such as regular updates and patches, risk assessments, and security audits, are necessary to address emerging threats and vulnerabilities. Collaboration and

information sharing within the cybersecurity community are vital for staying ahead of evolving threats and developing robust defenses. Additionally, the role of government and regulatory bodies in establishing cybersecurity standards and promoting a secure digital environment is crucial for enhancing operating system security on a broader scale. Through collective efforts, including collaboration, proactive measures, and regulatory support, we can effectively protect operating systems and uphold the security of data and operations.

Supplementary Information

The various original data sources some of which are not all publicly available, because they contain various types of private information. The available platform provided data sources that support the exploration findings and information of the research investigations are referenced where appropriate.

Acknowledgments

The author would like to acknowledge and thank the GOOGLE Deep Mind Research with its associated pre-prints access platforms. This research exploration was investigated under the platform provided by GOOGLE Deep Mind which is under the support of the GOOGLE Research and the GOOGLE Research Publications within the GOOGLE Gemini platform. Using their provided platform of datasets and database associated files with digital software layouts consisting of free web access to a large collection of recorded models that are found within research access and its related open-source software distributions which is the implementation for the proposed research exploration that was undergone and set in motion. There are many data sources some of which are resourced and retrieved from a wide variety of GOOGLE service domains as well. All the data sources which have been included and retrieved for this research are identified, mentioned and referenced where appropriate.

Declarations

- Funding

No Funding was provided for the conduction of this research.

- Conflict of interest/Competing interests

There are no Conflict of Interest or any type of Competing Interests for this research.

- Ethics approval

The author declares no competing interests for this research.

- Consent to participate

The author has read and approved the manuscript and have agreed to its publication.

- Consent for publication

The author has read and approved the manuscript and have agreed to its publication.

- Availability of data and materials

The various original data sources some of which are not all publicly available, because they contain various types of private information. The available platform provided data sources that support the exploration findings and information of the research investigations are referenced where appropriate.

- Code availability

Mentioned in details within the Acknowledgements section.

- Authors' contributions

Described in details within the Acknowledgements section.

References

1. Quissanga FC. Characterization of cellular mobile operating systems: Android, Symbian, iphone and Windows phone. Project, Design and Management. 2019;1(2):80-83. DOI: 10.35992/pdm.v1i2.200
2. Creswell JW. Research design qualitative, quantitative and mixed methods. 2010. Available from: https://edisciplinas.usp.br/pluginfile.php/696271/mod_resource/content/1/Creswell.pdf.
3. Chaer G, Diniz R, Ribeiro E. The questionnaire technique in educational research: The questionnaire in empirical issues. Evidência, Araxá. 2011;7(7):251-266. Available from: http://www.educadores.diaadia.pr.gov.br/arquivos/File/maio2013/sociologi a_artigos/pesqusia_social.pdf
4. Quissanga FC. Characterization of cellular mobile operating systems: Android, Symbian, iphone and Windows phone. Project, Design and Management. 2019;1(2):77. DOI: 10.35992/pdm.v1i2.200
5. Futurelearn. The National Cyber Security Centre– The Open University; 2019. Available from: https://www.futurelearn.com/courses/introduction-to-cybersecurity/17/steps/565630
6. Martinelli H. Vírus de celular: Estudo e classificação para um protótipo de defesa: ANEXO B: Código do vírus Cabir. Brasil- Porto Alegre: Uniritter; 2008. Retrieved from: http://www.uniritter.edu.br/graduacao/informatica/sistemas/downloads/tcc2k8/TCC%202%20final(Horst).pdf
7. Le Thanh H. Analysis of malware families on android mobiles: Detection characteristics recognizable by ordinary

phone users and how to fix it. Journal of Information Security. 2013;4(4):12. Article ID: 36799. DOI: 10.4236/jis.2013.44024

8. Leite AC, Reis HM. Comparativo entre sistemas operativos móveis - Android x iOS. 2017. p. 7. Available from: https://simtec.fatectq.edu.br/index.php/simtec/article/view/253/236
9. Pandya VR, Mark S. iPhone security analysis: Security analysis. Journal of Information Security. 2010;1:74-87. doi: 10.4236/jis.2010.12009. Published Online October 2010. Available from: http://www.SciRP.org/journal/jis
10. Terra. Panama papers. The Interne. 2016. Available from: https://www.terra.com.br/noticias/mundo/panama-papers-geram-denuncias-e-investigacoes-em-todo-o-mundo,814039f797239995dea030884e41f8faakajlviv.html
11. Ferreira FC. De Sistemas operativos. Esab - Escola Superior Aberta do Brasil Ltda. First edition: 2008. Available from: http://www.esab.edu.br.
12. Medranda, J. M. A. Enfoque de las redes sociales en estudantes universitários. 2017. p. 192. Available from: https://dialnet.unirioja.es/servlet/articulo?codigo=6102844.
13. Tumejormovil Comparison of the most used mobile operating systems(Android, iOS, Windows Phone): Operating System. 2019. Available from: https://tumejormovil.com/operative-systems/.
14. Rina. A comparative analysis of mobile operating systems. 2018;6(12):70 E-ISSN: 2347-2693. Available from: https://www.ijcseonline.org/pub_paper/11-IJCSE-05378.pdf
15. Haseeb A. Comprehensive and technical overview of Android and IOS OS. International Journal of Computer Sciences and Engineering. 2015;3(1):49-57 E-ISSN: 2347-2693. Available from: Comprehensive and Technical Overview of Android and IOS OS (ijcseonline.org)
16. Alvarez I. A study on Apple□s iOS operating system. kriativ-tech. Edição Nº 7 □ 28 de Agosto de 2018. ISSN
17. Print: 1646-9976 | ISSN Online: 2184-223X | DOI: 10.31112/kriativ-tech-2018-01-20
18. M. Gao, C. Wang and Z. Qian, "An Accurate Power-Sharing Control Method Based on Circulating-Current Power Phasor Model in Voltage-Source Inverter Parallel-Operation System," 2018.
19. R. A. Clarke and R. K. Knake, "Cyber war: the next threat to national security and what to do about it?," p. 290, 2010.
20. S. W. A. Hamdani, H. Abbas, A. R. Janjua and W. B. Shahid, "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons," 2021.
21. J. Harry Katzan, "Cybersecurity Service Model. Journal of Service Science," p. 77, 2012.
22. National Cyber Security Centre, "What is an antivirus product? Do I need one?," 21 January 2019. [Online]. Available: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product. [Accessed 23 June 2023].
23. B. S. D. S. Negara, "Tip Singkat & Praktis di Dunia Siber dari BSSN Untuk Masyarakat," 2018, p. 10.
24. Aamir M, Rizvi SSH, Hashmani MA, Zubair M, Ahmad J. Machine learning classification of port scanning and DDoS attacks: A comparative analysis. Mehran University Research Journal of Engineering and Technology. 2021;40(1):215□229. doi: 10.22581/muet1982.2101.19. [CrossRef] [Google Scholar]
25. Aassal A, El S, Baki A. Das, Verma RM. An in-depth benchmarking and evaluation of phishing detection research for security needs. IEEE Access. 2020;8:22170□22192. doi: 10.1109/ACCESS.2020.2969780. [CrossRef] [Google Scholar]
26. Abu Al-Haija Q, Zein-Sabatto S. An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics. 2020;9(12):26. doi: 10.3390/electronics9122152. [CrossRef] [Google Scholar]
27. Akhtar, Z.B. Securing Operating Systems (OS): A Comprehensive Approach to Security with Best Practices and Techniques. International Journal of Advanced Network, Monitoring and Controls, 2024, Sciendo, vol. 9 no. 1, pp. 100-111. https://doi.org/10.2478/ijanmc-2024-0010
28. Akhtar, Z.B. & Rawol, A.T. Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective. International Journal of Advanced Network, Monitoring and Controls, 2024, Sciendo, vol. 9 no. 2, pp. 11-22. https://doi.org/10.2478/ijanmc-2024-0012
29. Z. Bin Akhtar, "Artificial Intelligence (AI) within the Realm of Cyber Security," Insight. Electr. Electron. Eng., vol. 1, no. 1, pp. 1-11, 2024.
30. Akhtar, Z. B., & Rawol, A. T. (2024). Harnessing artificial intelligence (AI) for cybersecurity: Challenges, opportunities, risks, future directions. *Computing and Artificial Intelligence*, *2*(2), 1485. https://doi.org/10.59400/cai.v2i2.1485