ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II

JAN – FEB 2025

Original Research Article

THE IMPORTANCE OF ANTIVIRUS APPLICATIONS FOR SMARTPHONES IN THE CONTEXT OF CYBER SECURITY AND MOBILE THREATS

**** Sachin Vasant Dorage***

** System Administrator, IT Department, Oriental College of Pharmacy, Navi Mumbai, Maharashtra, India.*

Abstract:

Smartphones are increasingly serving as a vital tool for efficiently accessing, locating, and sharing information. However, the widespread availability of this information has led to a rise in cyber-attacks. Currently, cyber threats encompass a range of issues, including Trojans, viruses, botnets, and various toolkits. Alarmingly, 96% of smartphones lack pre-installed security software, creating a significant vulnerability that malicious cyber attackers can exploit across popular devices such as Android, iPhone, and Blackberry. Unlike traditional personal computers (PCs), which typically have security measures like firewalls, antivirus programs, and encryption, smartphones are often left unprotected. Additionally, smartphones are more susceptible to attacks as they are increasingly used for personal tasks. Today, users engage in activities such as emailing, utilizing social media platforms (like Facebook and Twitter), downloading applications, and online shopping. They also conduct financial transactions, including purchasing goods, redeeming coupons and tickets, banking, and processing point-of-sale payments. These monetary transactions are particularly appealing to cyber attackers, as they can potentially access sensitive bank account information by compromising a user's smartphone. Furthermore, the compact size and portability of smartphones enhance their convenience for personal tasks, which inadvertently creates opportunities for cyber attackers to infiltrate personal data. Therefore, this paper explores the necessity of establishing a national security policy specifically designed for mobile devices to safeguard sensitive personal information.

Key Words: *Cyber Security, Smart Phone, Banking, National Security Policy.*

Introduction:

At present, smartphones have become the favored devices for activities such as web browsing, emailing, engaging with social media, and conducting online purchases. Their compact size allows for convenient transport in pockets, purses, or briefcases. However, the widespread use of smartphones has created opportunities for cybercriminals. The operating systems of these devices typically lack the security software necessary to safeguard user data. Unlike traditional security measures available on personal computers, including firewalls, antivirus programs, and encryption, such protections are not yet implemented on smartphones (Dawson Maurice, 2016). Mobile phone operating systems are not updated as regularly as those for personal computers, creating a

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II

JAN – FEB 2025

Original Research Article

security vulnerability that cyber attackers can exploit. A notable instance of this vulnerability occurred during the 2011 Valentine's Day attack, where cyber attackers distributed a mobile picture-sharing application that secretly transmitted premium-rate text messages from users' devices. This incident underscores the necessity of implementing a robust security policy for mobile phones (Dawson Maurice, 2016).

Electronic Commerce (E-Commerce) Applications and Social Networking:

Numerous individuals depend on their smartphones for a variety of tasks, including sending emails and storing contact details, passwords, and other sensitive information. Furthermore, smartphones have become the preferred device for engaging in social networking, making mobile applications for platforms such as Facebook, Twitter, and Google+ potential targets for cybercriminals seeking to extract personal information from unsuspecting users (Mansour Alsaleh, 2017). Social networking sites contain an abundance of personal data, which is why malicious applications that exploit these platforms to steal information can have dire repercussions. Recently, mobile commerce, or M-Commerce, has surged in popularity within our society. A significant number of smartphone users are now able to perform financial transactions, such as purchasing goods and applications, redeeming coupons and tickets, as well as banking and processing point-of-sale payments. While these smartphone capabilities offer convenience to users, they also present opportunities for malicious cyber attackers. Consequently, there exists a demand for cybersecurity software specifically tailored for mobile operating systems.

Potential Outcomes of Cyber Attacks on Smartphones:

The repercussions of a cyber-attack targeting a smartphone can be equally harmful, if not more so, than those affecting a personal computer. Patrick Traynor, a researcher and assistant professor at the Georgia Tech School of Computer Science, notes that mobile applications depend on the browser for their functionality. Consequently, it is anticipated that the frequency of web-based attacks on smartphones will rise over the course of the year (Sarthak Sampad Roy, 2023). Traynor further emphasizes that IT professionals, computer scientists, and engineers must continue to investigate the differences between mobile and traditional desktop browsers in order to gain a comprehensive understanding of how to mitigate cyber-attacks.

Figure 1. Potential outcomes of cyber-attacks on smartphones

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II

JAN – FEB 2025

Original Research Article

Challenges Associated with A Mobile Browser:

A notable cyber security challenge for mobile devices is the limited screen size. For instance, the web address bar, which becomes visible when a user opens a browser app, tends to vanish after a few seconds on smartphones due to this constraint (Traynor, 2012). This typically serves as the primary line of defense in cybersecurity. Verifying the Uniform Resource Locator (URL) of a website is the initial method by which users can confirm their presence on a legitimate site. Additionally, locating SSL certificates for a website can often be more challenging when using a mobile phone browser (Traynor, 2012).

Figure 2. Challenges associated with a mobile browser (AppStudio, 2021).

Widely Used Mobile Operating Systems – IOS and LINUX

Apple introduced iOS, originally known as iPhone OS, in 2007 alongside the launch of the iPhone, marking its entry into the mobile phone industry (David Barrera, 2011). Currently, the iOS platform operates not only on the iPhone but also on the iPod Touch and iPad. Developers at Apple create applications designed to function across all iOS devices (David Barrera, 2011). The widespread appeal of Apple's iOS can be attributed to its user-friendly interface, which features onscreen interactive menus, 2D and 3D graphics, location services, and essential operating system capabilities such as threading and network sockets (David Barrera, 2011).

Mobile applications have become essential across various sectors, driving growth and development for numerous enterprises. The rising demand for tailored app development and accessible app creation tools serves as a significant indicator of the increasing popularity and necessity of mobile applications. In the realm of mobile operating systems, Android and iOS emerge as the primary contenders, collectively dominating the vast majority of the market. While Android boasts a broader user base, iOS is often recognized for its esteemed reputation among users. In this discussion, we will examine the market share of these two industry leaders and explore relevant statistics and insights regarding their performance. Let us proceed to analyze the current standing of these mobile operating systems in relation to one another (statistics, 2024).

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

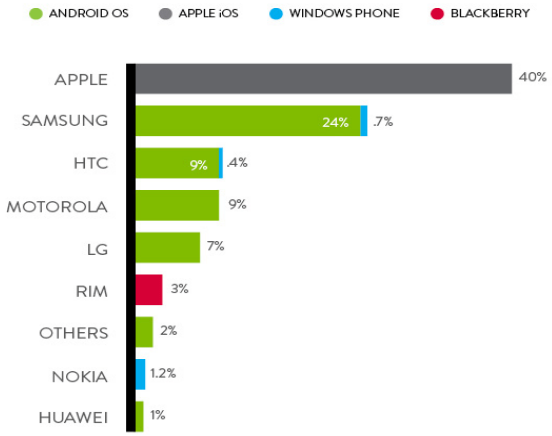
VOLUME–XII, SPECIAL ISSUES–II

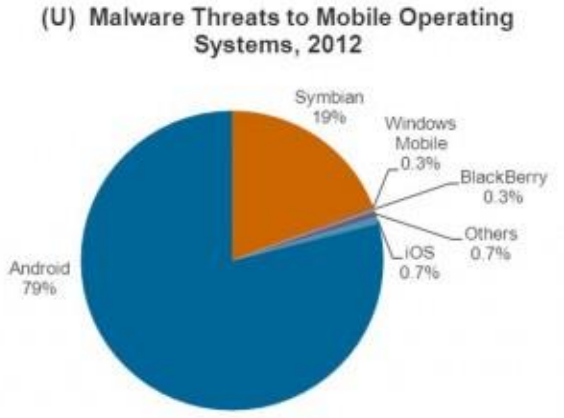
JAN – FEB 2025

Original Research Article

Regarding costs, most Linux distributions are available at no charge. However, some may incur fees for updates or support tailored to specific requirements, such as modifications for server hosting. The Linux operating system employs a package management system that streamlines the installation, configuration, upgrading, and removal of software packages. The most prevalent package management systems in Linux distributions include Debian, Red Hat Package Manager (RPM), Knoppix, and netpkg. Among the most widely used Linux distributions for mobile devices are Android, iOS, and Ubuntu.

Figure 3. Widely Used Mobile Operating Systems – IOS and Linux (Nielsen, 2013).





MALWARE INCIDENTS TARGETING SMARTPHONE OPERATING SYSTEMS

Malware designed to exploit smartphone operating systems is continuously advancing. A notable instance is "Zeus-in-the-Mobile" (ZitMo), a type of malware prevalent among Android users. ZitMo specifically aimed at banking applications on Android devices, attempting to circumvent two-factor authentication, steal user credentials, and ultimately access bank accounts and funds (Traynor, 2012). This represents just one type of cyber threat that IT professionals are actively working to mitigate. It is increasingly recognized that mobile devices may serve as a new avenue for targeting network and critical systems. The report indicates that smartphones are particularly effective for disseminating malware due to their substantial storage capabilities. A potential scenario illustrating a cyber-attack on a corporate network involves the introduction of malware through a smartphone. For instance, a skilled cyber attacker could develop code to gain remote access to wireless connectivity features and embed malware within the mobile device. If this smartphone subsequently connects to a corporate network such as when the user charges it on a company computer the malware could then compromise the network. IT professionals are keen to avert such attacks, as the economic ramifications could be devastating (Traynor, 2012). Therefore, establishing a national security standard for mobile devices is essential to safeguard personal data.

Figure 4. Malware Incidents Targeting Smartphone Operating Systems (Threats to Mobile Devices Using the Android Operating System, n.d.)

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II JAN – FEB 2025

Original Research Article

The Android Operating System:

Android is an open-source application execution environment that encompasses an operating system, an application framework, and essential applications. Initially developed and launched by Android Inc., Android aimed to create a user-friendly, accessible mobile development platform. This open-source framework is designed with the user in mind, offering a wide range of development tools and features. However, the open-development aspect also presents challenges in securing sensitive user information and safeguarding against malicious threats, such as phishing applications that deceive users into revealing their financial details and credentials while navigating fraudulent websites that mimic legitimate banking sites (Asaf Shabtai, 2010).

The Android operating system made its debut in October 2008 with the T-Mobile 1G, quickly gaining traction among major telecommunications providers in the U.S. and Europe due to its extensive capabilities, which include core applications like email, web browsing, and multimedia messaging, as well as entertainment features and services such as camera functionality and Bluetooth connectivity. This has contributed to Android's appeal among developers, as its open-source nature allows for the creation and programming of sophisticated applications at the foundational level of the operating system. Since its launch, Android has seen numerous updates, with the latest being Android 2.2. This version introduces a host of new and enhanced features aimed at improving user and developer productivity, including significant speed enhancements (with CPU performance increasing by 2-5 times) and improved browsing capabilities (utilizing version 8 engine for 2-3 times faster JavaScript-heavy page loading). Additionally, this update enhances security measures, enabling users to unlock their devices with a password policy and providing the option to erase data remotely in the event of theft or loss (Asaf Shabtai, 2010).

The Security Framework of Android:

Android operates as a multi-process system, with each application and certain system components executing within their own distinct processes. The inherent security features of Linux establish boundaries between applications and the system at the process level, assigning user and group IDs to these applications. A permission mechanism, known as permission labels, imposes restrictions on the actions that applications can undertake, utilizing access control to manage these capabilities. This mechanism is highly detailed, regulating the specific operations that individual processes may execute (Asaf Shabtai, 2010). Permission labels form an integral part of a security policy designed to limit access to various components within an application. Android employs these security policies to assess and determine whether to approve or reject permissions for applications installed on the Android operating system.

The existing security policies exhibit significant limitations, as they fail to clearly define which applications are granted specific rights or permissions. This ambiguity arises from their dependence on users and the operating system to make such determinations. Consequently, there is an inherent risk of allowing potentially harmful applications to access sensitive information on the device. For instance, consider a hypothetical scenario involving a "PayPal service" operating on Android. Various applications, including web browsers, email clients, software marketplaces, and music players, utilize this PayPal service for transactions. In this context, the PayPal

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

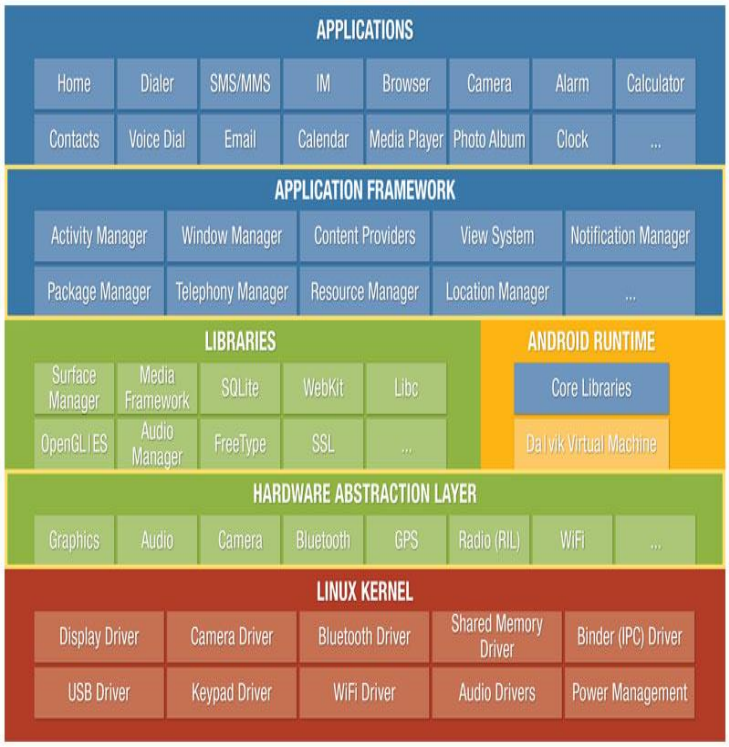
VOLUME–XII, SPECIAL ISSUES–II

JAN – FEB 2025

Original Research Article

service functions as an application that requires permissions to be granted to other applications that interact with its interfaces (Ontang). However, it remains uncertain whether the PayPal application in question is genuine, as there is no mechanism to verify its authenticity against a malicious counterpart. Furthermore, Android lacks the necessary security protocols to ascertain and regulate the conditions under which permissions are granted, including the timing, location, and recipients of such permissions.

Figure 5. The Security Framework of Android (iOS), 2024)



Android Permissions Management:

Android employs a permission system to regulate user actions within applications. This is facilitated through manifest permissions, which grant applications the ability to operate independently from one another and from the operating system. This design enhances security by ensuring that the actions of one application do not disrupt or affect the functionality of others. For instance, users sending emails are typically restricted from executing operations in other applications, such as accessing files, which could negatively influence the email application. This isolation is achieved through the "sandbox" model, where each application is allocated the essential functions required to execute its own processes. However, if an application requires additional functions not provided by its sandbox, it may potentially interfere with other processes and request those necessary functions. This ability for applications to seek permissions beyond their sandbox limitations poses a risk to Android devices, as it creates opportunities for malware to gain access to sensitive information and install Injurious software (Francesco Di Cerbo, 2010).

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II JAN – FEB 2025

Original Research Article

Measures to Safeguard Mobile Devices:

When selecting a mobile phone, it is essential to take into account its security features:

- Enhance the device's security settings.
- Ensure that web accounts are configured to utilize secure connections.
- Refrain from clicking on links provided in suspicious emails or text messages.
- Minimize the exposure of your mobile phone number.
- Thoughtfully evaluate the information you wish to store on the device.
- Exercise discretion when choosing and installing applications.
- Maintain physical possession of the device, particularly in public or semi-public areas.
- Disable any interfaces that are not in active use, such as Bluetooth, infrared, or Wi-Fi.
- Set Bluetooth-enabled devices to non-discoverable mode.
- Avoid connecting to unfamiliar Wi-Fi networks and refrain from using public Wi-Fi hotspots.
- Erase all data from the device before disposing of it.
- Exercise caution when engaging with social networking applications.
- Avoid "rooting" or "jailbreaking" the device.

Conclusion:

There are viable solutions to the pervasive issue of cybersecurity concerning smartphones. When society recognizes that cybersecurity threats pose risks to not only individual users but also to the community at large, the groundwork for effective solutions can commence. The significance of data is on the rise, potentially surpassing that of traditional currency. Therefore, it is essential to cultivate a culture of cybersecurity, as this challenge is complex and technology continues to advance rapidly.

References:

1. *AppStudio. (2021, Dec 20). appstudio. Retrieved from https://www.appstudio.ca/: https://www.appstudio.ca/blog/8-major-challenges-of-mobile-website-optimization/*
2. *Asaf Shabtai, Y. F. (2010). Google Android: A Comprehensive Security Assessment. IEEE Security and Privacy Magazine, IEEE Xplore, 35 - 44. doi:DOI:10.1109/MSP.2010.2*
3. *David Barrera, P. C. (2011). Secure Software Installation on Smartphones. IEEE Security and Privacy Magazine, 9(3):42-48. doi:DOI:10.1109/MSP.2010.202*
4. *Dawson Maurice, W. J. (2016). Mobile Devices: The Case for Cyber Security Hardened Systems. Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications, 1103. doi:10.4018/978-1-4666-8751-6.ch047*
5. *Francesco Di Cerbo, A. G. (2010). Detection of malicious applications on Android OS. IWCF'10: Proceedings of the 4th international conference on Computational forensics, 138 - 149.*
6. *iOS), M. o. (2024, Augest 15). Mobile operating systems (Android and iOS). Retrieved from https://library.fiveable.me/: https://library.fiveable.me/operating-systems/unit-10/mobile-operating-systems-android-ios/study-guide/w4eZgDk0OqPNdwM8*

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

VOLUME–XII, SPECIAL ISSUES–II JAN – FEB 2025

Original Research Article

7. *Mansour Alsaleh, N. A. (2017, March 17). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. National library of medicine national center for the biotechnology information. doi:10.1371/journal.pone.0173284*
8. *Nielsen. (2013). www.nielsen.com. Retrieved from www.nielsen.com: https://www.nielsen.com/insights/2013/whos-winning-the-u-s-smartphone-market/*
9. *Ontang, M. M. (n.d.). Semantically rich applicationcentric security in Android. Retrieved from Proceedings of teh 25th Annual Computer Security Applciations Conference (ACSAC '09).*
10. *Sarthak Sampad Roy, M. P. (2023). A HYPOTHETICAL ALALYSIS OF CYBER CRIME AND IT'S IMPACT. International Journal of Advance Research and Innovative Ideas in Education.*
11. *statistics, M. O. (2024, January 9). www.appmysite.com. Retrieved from www.appmysite.com: https://appmysite.com/blog/android-vs-ios-mobile-operating-system-market-share-statistics-you-must-know/*
12. *Threats to Mobile Devices Using the Android Operating System. (n.d.). Retrieved from www.networksplusco.com: https://www.networksplusco.com/threats-to-mobile-devices-using-the-android-operating-system/*
13. *Traynor, P. A. (2012). Emerging Cyber Threats Report 2012,. Georgia Tech Information Security Center, Atlanta, GA.*

Cite This Article:

***Dorage S. V.* (2025).** *The Importance of Antivirus Applications for Smartphones in the Context of Cyber Security and Mobile Threats.* **In Educreator Research Journal: Vol. XII (Issue I),** pp. 83–90.