Security Vulnerabilities in Mobile Operating Systems Used in IoT Devices: An Examination of Current Challenges and Countermeasures

Isain Cortes Jr.
Old Dominion University

Security Vulnerabilities in Mobile Operating Systems Used in IoT Devices: An Examination of Current Challenges and Countermeasures

Isain Cortes, Jr.

Old Dominion University School of Cybersecurity

COVA CCI Undergraduate Research Program

(November 2024)

Security Vulnerabilities in Mobile Operating Systems Used in IoT Devices: An Examination of Current Challenges and Countermeasures

Abstract

The proliferation of Internet of Things (IoT) devices has led to increased reliance on mobile operating systems (OS) such as Android, iOS, Windows, and Blackberry (RIM) to control and interact with these devices across diverse environments. This research explores the most common security vulnerabilities across these platforms, including malware, insecure data storage, insufficient encryption practices, and potential weaknesses within app ecosystems. The study provides a comprehensive look at Android and iOS, while also examining Windows and Blackberry for their roles in specific IoT applications. By reviewing existing vulnerabilities, analyzing recent data on security incidents, and assessing the effectiveness of current countermeasures, this research highlights critical gaps in OS security that must be addressed to protect IoT-integrated devices. The findings suggest the need for enhanced, standardized security frameworks that can adapt to the rapidly evolving digital landscape, with implications for developers, users, and policymakers focused on securing the future of IoT.

Definition

According to Ahvanooey, Li, Rabbani, Rajput (2017), a smartphone OS (or Mobile OS), is a system software which is able to run on smart gadgets (such as smartphones, tablets, phablets and other support devices), that allows it to run other applications developed for its platform.

1. Introduction

The rapid development of Internet of Things (IoT) devices has fundamentally changed the way individuals and organizations interact with technology. These interconnected devices, which range from smart thermostats and fitness trackers to industrial machines and medical

devices, rely heavily on mobile operating systems like Android, iOS, Windows, and Blackberry (RIM) for their functionality and management.

As the number of IoT devices continue to grow, the security of the mobile OS platforms that interface with these devices become increasingly critical. Vulnerabilities within these OS platforms can expose devices to cyberattacks, data breaches, unauthorized access, and manipulation, threatening user privacy and system integrity. In order to make commercial IoT devices more resilient to cyberattacks, security should be taken into account right from the design stage of new products (Meneghello, Calor, Zucchetto, Polese, Zanella 2019).

Currently the majority of internet users are connected via a smartphones, tablets, and PCs (Ahvanooey, Li, Rabbani, Rajput 2017). According to a report by ComScore, as depicted in Figure 1, two distinct groups of internet users have emerged: "desktop PC users" and "smartphone users." As of March 2015, over 1.8 billion smartphone users were reported, outnumbering desktop users. This shift highlights the increasing dominance of smartphones in recent years, making mobile operating systems a critical element in the functioning and security of IoT devices.

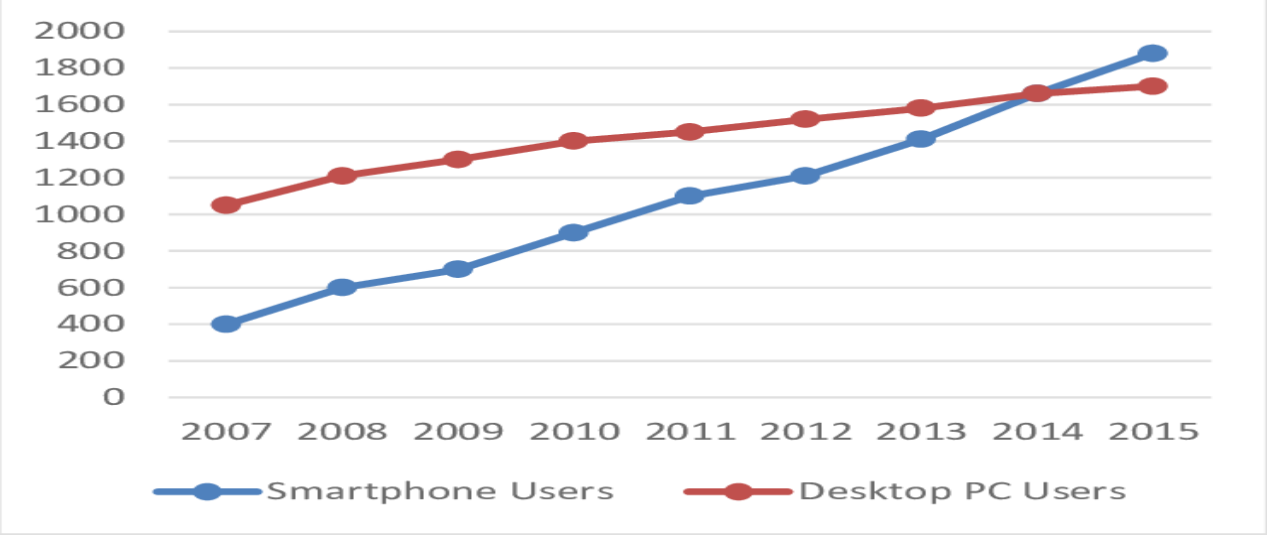

Fig. 1. Number of internet users (millions)

Android and iOS dominate the IoT market, particularly in consumer devices, with Android holding the largest global market share. However, these platforms are not without their own security risks, including malware, unsecured data storage, and issues with app permissions and encryption. Windows and Blackberry, though less prominent in IoT today, continue to play an important role in enterprise and industrial sectors where IoT applications require specific security features. Although these platforms are often regarded as more secure, they are not immune to vulnerabilities that can jeopardize the security of IoT ecosystems. Understanding the security vulnerabilities across these platforms is essential for developing stronger defenses and improving the overall security posture of IoT devices.

Research Question

What are the most common security vulnerabilities across major mobile operating systems used in IoT devices?

With the growing use of mobile OS platforms to manage and control IoT systems, understanding these weaknesses is critical for improving the security of interconnected devices and protecting sensitive user data. The study will explore a variety of security concerns, including malware susceptibility, data storage issues, insufficient encryption, and vulnerabilities within the app ecosystems. By evaluating the current state of mobile OS security, the research aims to provide insights into the most pressing security gaps and offer recommendations for mitigating risks in IoT environments.

Scope of the Study

The scope of this research primarily focuses on the two dominant mobile operating systems in the IoT market: Android and iOS. These platforms are integral to the vast majority of

consumer IoT devices and represent the most significant areas of concern in terms of security. However, the study also includes a brief examination of Windows and Blackberry (RIM), which continue to serve niche markets, especially in enterprise IoT applications. By exploring the vulnerabilities and security practices of these four mobile OS platforms, the research aims to provide a well-rounded analysis of the current state of IoT security across different types of devices and environments.

2. Security Vulnerabilities in Mobile Operating Systems

Android

Android was designed with openness in mind (Ahvanooey, Li, Rabbani, Rajput 2017), especially in IoT devices. However, its openness introduces several security challenges. The large number of available applications increases the potential attack surface, as very few of these applications might have bugs which can be abused by hackers or viral infections (Adekotujo, Odumabo, Adedokun, & Aiyeniko, 2020). Hackers can utilize reverse engineering techniques to obtain sensitive information from the open-source apps and manipulate these apps for their malicious purposes through Google Play. Android devices can be unstable and prone to crashes, particularly if frequent system updates are not properly managed, leaving the device exposed to security risks. Rooting, a process that grants administrative access to the system can present a security concern. While rooting offers advanced features, it bypasses Android's built-in security mechanisms, making the device more vulnerable to attacks. Many Android applications require an internet connection, which increases the potential for data leakage if proper security protocols are not in place. Poor battery management, especially when security features are running in the background, can further compromise the device's protection, particularly when it enters low-power mode (Adekotujo, Odumabo, Adedokun, & Aiyeniko, 2020).

iOS

While known for its relatively secure ecosystem, it is not immune to security vulnerabilities. Apple's stringent control over hardware and software integration can limit the operability of the system (Adekotujo, Odumabo, Adedokun, & Aiyeniko, 2020). Additionally, jailbreaking is a common practice that allows users to bypass Apple's restrictions and install unauthorized apps or make system modifications. While jailbreaking can enhance device functionality, it bypasses the security of iOS and permits all the apps, including malware, to access the data which is assigned by other apps (Ahvanooey, Li, Rabbani, Rajput 2017).

Windows

Windows operating systems, particularly Vista and Windows 7, come with several security challenges. One of the issues is the need to purchase antivirus programs that require frequent activation, either manually or automatically. Although free antivirus options exist, they come with limitations (Adekotujo, Odumabo, Adedokun, & Aiyeniko, 2020). Additionally, Windows operating systems demand significant system resources, including registers, cache, main memory, processor, and disk space, which can slow down the system's performance. Another concern is the high cost of purchasing a Windows operating system, making it unaffordable for many users. This often leads to the cracking of the software and the availability of pirated versions (Adekotujo, Odumabo, Adedokun, & Aiyeniko, 2020).

Blackberry (RIM)

Once a leader in mobile security, Blackberry faces unique challenges in the modern IoT landscape. Blackberry 10.x provided some key security features such as platform security, secure device management, data in transmission security, app security, etc. (Ahvanooey, Li, Rabbani,

Rajput 2017). However, with the introduction of the ability to run Android apps, Android malware has become a significant concern for Blackberry devices. Malware that targets Android OS vulnerabilities can easily affect Blackberry 10.x systems, particularly if users download apps from untrusted sources.

3. Case Studies of IoT Security Incidents and Comparative Analysis

Android Case Studies

Writers of mobile malware are targeting mostly the Android platform. In 2013, the U.S. Department of Homeland Security stated in a report that the Android platform accounts for 79% of all mobile malware (Mohamed, Patel 2015). With Android being an open-source platform, it is a popular target for cybercriminals due to its widespread use and the large attack surface created by the extensive app ecosystem. Over the years, several mobile malware families have emerged, each designed to exploit vulnerabilities within the Android operating system. These malware strains often target personal and financial data, while others are designed to take control of infected devices for malicious purposes. Below are some of the most notable Android malware families discovered between 2016 and 2017:

Name	Malicious Activities
Hummingbad	This virus steals banking credentials and bypasses encrypted email containers used by enterprises.
Pegasus	This spyware allows hackers to control the victim's device, enabling them to steal sensitive information.
Swearing	This Trojan steals bank credentials and other sensitive information from its users.
Gooligan	This rootkit steals authentication tokens and provides access to data from Google Play, Gmail, Google Photos, Google Drive, and more.
FalseGuide	This malware generates a silent botnet from the victim’s device, which is used for adware or other malicious purposes.
Triada	This malware uses a backdoor to infect OS processes and provides remote access for stealing money from users.
Hiddad	This Trojan allows hackers to gain access to sensitive user information.

Ztorg	This Trojan installs hidden apps on the victim's device and steals login credentials.
DressCode	This malware creates a botnet that uses compromised IP addresses to generate false network traffic, making revenue for the attackers.

With these threats in mind, Android has made in efforts in its security and does present key security features. The Linux kernel underpins Android's security with a user-based permission model, secure inter-process communication, and process isolation. A mandatory application sandbox assigns each app a unique user ID, isolating it from others to limit cross-app interference. Android also employs application signing, which informs users of app permissions during installation, and user-granted permissions, providing greater control over access. These measures help Android balance its open-source flexibility with robust security against IoT-related threats.

iOS Case Studies

Though iOS is known for its strong security protocols, it too like Android, faced attacks from major malware such as Hummingbad, Pegasus, and FalseGuide, resulting in stolen bank credentials, remotely controlled iOS devices, and silent botnets exploiting them for adware and other malicious purposes. In addition to these, a famous incident involving XcodeGhost in 2015 demonstrated the global impact of compromised development tools on the iOS platform. This malware infected 39 iOS apps, including some of the most popular applications in China and other countries, comprising hundreds of millions of users (Xiao 2015). The compromised apps ranged from instant messaging platforms, banking apps, maps, stock trading applications, social networking services, and games. According to Mohamed and Patel (2015), statistics by Common Vulnerabilities and Exposures (CVE) claimed that 408 of vulnerabilities were discovered in the iOS operating system during 2007–2014 in its various versions. Also stating from Symantec, the

time that Apple took on average to patch a vulnerability was 12 days from the time it was reported. Four days longer than Android's average vulnerability patch time.

In terms of security architecture, iOS offers a comprehensive set of tools to protect users and apps. It uses Common Data Security Architecture (CDSA) integrated into the BSD kernel, which manages file access permissions and supports features like encryption, secure data storage, and authentication. A key security mechanism is app sandboxing which isolates each app to prevent unauthorized access to data. iOS also controls app permissions, limiting access to essential resources without user intervention, although users may grant permissions for actions like notifications, location data, and messaging. While these protections are robust, the constant evolution of malware techniques requires Apple to stay one step ahead, continuously strengthening iOS defenses to ensure user security.

Windows Case Studies

Windows has been a significant player in the mobile OS market, though its mobile platform saw limited success as 0.5% of market share belonged to this OS in 2016 (Ahvanooey, Li, Rabbani, Rajput 2017). One of the most notable events affecting Windows in recent history was the WannaCry ransomware attack in 2017. This attack exploited the SMB CVE-2017-0145 vulnerability with EternalBlue via internet facing TCP port445, executing DoublePulsar backdoor on the infected device (Aljaidi, Alsarhan, Samara, Alazaidah, Almatarneh, Khalid 2022), impacting thousands of devices.

Although Microsoft discontinued the Windows Phone in 2017, Windows still integrated notable security features into its mobile devices. Windows 10 Mobile shared many security mechanisms with Windows 10 for PCs, including Windows Hello for Business for secure multi-

factor authentication, Windows Information Protection to separate corporate and personal data, and malware resistance with multi-layered protections to reduce malware risks.

Blackberry (RIM) Case Studies

As mentioned earlier, the integration of running Android apps on Blackberry devices introduced a significant security concern. Android malware, which exploits vulnerabilities in the Android OS, can easily affect Blackberry 10.x systems, particularly when users download apps from untrusted sources. While the new compatibility feature was beneficial in some ways, it exposed Blackberry users to the risks associated with Android malware. Blackberry notably experienced a major outage in 2011, impacting 70 million users worldwide, which RIM later called a, “core switch failure” (Arthur, Baxter-Reynolds 2011). This outage raised concerns about the reliability and security of Blackberry’s infrastructure.

Despite these challenges, Blackberry 10.x maintained strong security protocols. Powered by the QNX Neutrino RTOS, the system ensured the integrity of the OS and protected against malware, tampering, and data leakage. It offers users high levels of control over their information, allowing for secure separation of personal and professional data while enhancing productivity. The OS utilized strong encryption and authentication methods to ensure secure connections to networks, including BlackBerry’s infrastructure, VPNs, and Wi-Fi. These security features made BlackBerry 10.x a trusted platform, particularly in corporate and government sectors where data protection was critical.

Comparative Analysis of OS Security for IoT

When examining operating systems for Internet of Things (IoT) devices, security becomes the foremost concern due to the vast potential for data breaches, cyberattacks, and

unauthorized access. Both Android and iOS have emerged as dominant players in the IoT space, each bringing its own strengths and challenges when it comes to securing devices. While Windows and BlackBerry have strong security features in specific areas, their role in the broader IoT market is relatively limited compared to Android and iOS

With its open-source nature, Android offers significant flexibility, but this openness also creates a larger attack surface. The extensive app landscape, particularly through third-party app stores, exposes Android devices to more potential vulnerabilities. Although Android includes security measures such as app sandboxing, user-permission models, and the ability to update vulnerabilities regularly, the fragmented nature of its ecosystem means that some devices may not receive timely patches, leaving them more susceptible to exploits. Additionally, the reliance on external app stores makes it harder to ensure that all apps meet a consistent security standard, increasing the risk of encountering malicious software on IoT devices running Android.

In contrast, iOS takes a much more controlled approach, reducing the potential for malware attacks. The App Store's stringent app review process and Apple's emphasis on security through hardware features like secure boot processes and hardware encryption provide a robust defense against cyber threats. iOS devices also benefit from the Secure Enclave, which stores sensitive data like encryption keys and biometric data separately from the main OS, further securing IoT devices from unauthorized access. Additionally, Apple's consistent and rapid patching of vulnerabilities ensures that devices running iOS are often more protected against the latest threats, making it a preferred choice for environments that require enhanced data security.

While Windows has contributed security mechanisms like Windows Defender and secure boot for industrial and enterprise IoT, its presence in the broader IoT market is limited. Devices running Windows IoT are primarily focused on specific use cases, such as industrial control

systems, and typically encounter fewer threats from mobile-specific malware. However, it still faces traditional cyber risks, and its security features, while strong, do not match the adaptability offered by Android or the closed security system of iOS.

Similarly, BlackBerry is now focused primarily on enterprise security, offering strong protections through its QNX Neutrino RTOS. BlackBerry's reputation for security stems from its robust encryption and device management capabilities, making it an excellent choice for highly regulated sectors like government and healthcare. However, its reduced market presence in the general IoT ecosystem limits its applicability in a broader context. As a result, despite its high security measures, BlackBerry's limited adoption makes it less relevant for most IoT use cases.

As seen in Figure 2, the threat landscape for mobile OS security clearly reflects these trends. F-Secure security data shows that 99% of malicious attacks target Android devices, highlighting the platform's overwhelming share of the mobile malware market. Kaspersky security data shows Android as the primary target at 84.5%, followed by iOS at 11.69%, with Windows and BlackBerry receiving far fewer attacks at 2.5% and 0.5%, respectively.

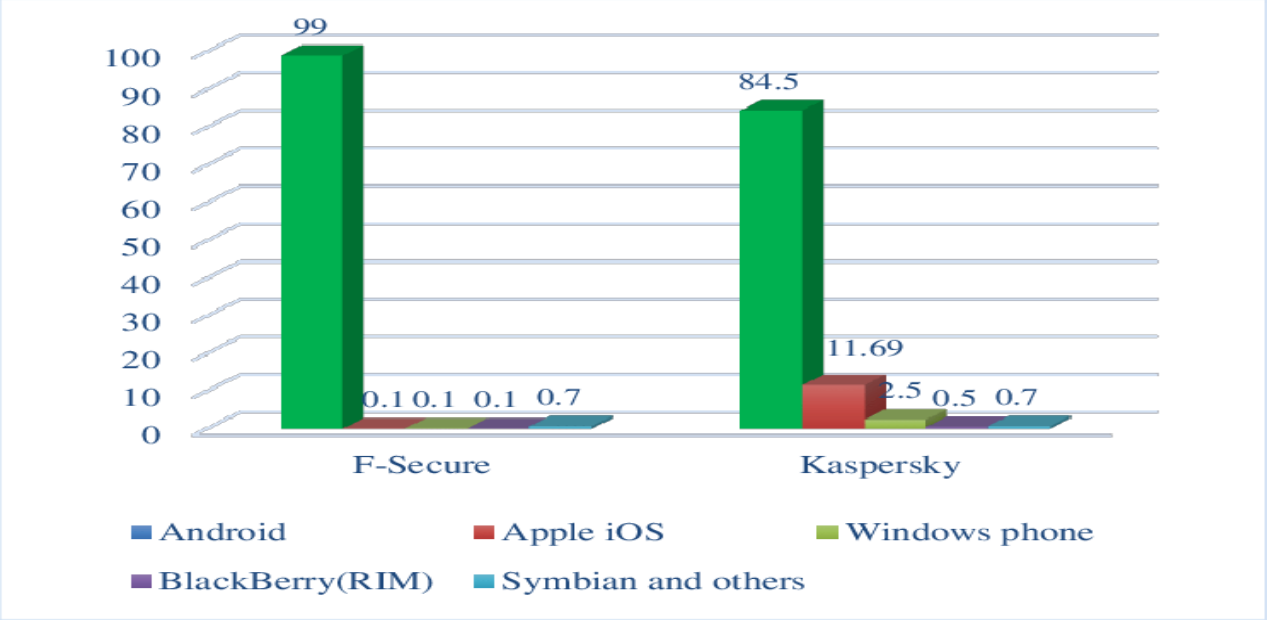

Fig. 2. Malware attacks on smartphone OSes

4. Countermeasures and Mitigations

To effectively mitigate vulnerabilities in mobile operating systems that interact with IoT devices, we can focus on implementing a range of security best practices. According to Weichbroth and Lysik (2020), the following 10 security measures are crucial for protecting user data and enhancing overall security within IoT ecosystems:

1. Make User Authentication the Highest Priority

Strong user authentication should be at the forefront of IoT security measures. Multi-factor authentication (MFA) is a highly effective way to ensure that only authorized individuals can access IoT systems and sensitive data. Requiring something beyond just a password, such as biometric verification or a one-time passcode, helps to mitigate the risk of unauthorized access.

2. Update Mobile Operating Systems and On-Board Applications with Security Patches

Timely updates are critical for addressing known vulnerabilities in both mobile operating systems and the applications running on IoT devices. Operating systems like Android and iOS regularly release patches to fix bugs and security flaws. However, it is essential for both manufacturers and users to prioritize these updates to ensure their devices are protected against emerging threats.

3. Back Up User Data on a Regular Basis

Backing up user data frequently is a simple yet effective way to prevent data loss, whether due to a cyberattack or device failure. Regular backups ensure that in the event of data corruption, deletion, or a ransomware attack, users can restore their data to a previous state, minimizing damage and downtime.

4. Utilize Encryption

Encryption is a cornerstone of data security. By encrypting sensitive data, it becomes unreadable to anyone who does not have the decryption key. Both Android and iOS use strong encryption protocols, such as full-disk encryption (FDE) and file-based encryption (FBE), to protect data on mobile devices. These mechanisms are essential for protecting user privacy, especially in the event that a device is lost or stolen.

5. Enable Remote Data Wipe

Remote data wipe functionality allows users to erase sensitive information from their devices in case of loss or theft. This feature ensures that even if a device falls into the wrong hands, the data remains secure. It is particularly useful for devices used in enterprise settings, where confidential business information is stored.

6. Disable Bluetooth and Wi-Fi When Not Needed

Leaving Bluetooth and Wi-Fi enabled when not in use can expose devices to unnecessary security risks. Both technologies can be exploited by attackers through vulnerabilities, enabling unauthorized access to a device. By disabling these features when not actively required, users reduce their attack surface and mitigate potential threats.

7. Be Aware of Social Engineering Techniques

Social engineering attacks, such as phishing, exploit human behavior to gain unauthorized access to systems or information. Users should be trained to recognize phishing attempts and avoid clicking on suspicious links or providing personal information via email or other communication methods. Awareness of these tactics is essential for preventing attackers from gaining access to sensitive data.

8. Avoid Jailbreaking Devices

Jailbreaking a device removes many of the security restrictions put in place by the operating system, leaving the device more vulnerable to malware and other malicious threats. Users should avoid jailbreaking their IoT devices, as it compromises the integrity of the device and reduces its ability to protect sensitive data.

9. Grant Only Necessary Permissions to Applications

Mobile applications often request permissions to access various features of a device, such as the camera, microphone, or location. Users should be mindful of granting only those permissions necessary for the app to function properly. Limiting app permissions helps to protect user privacy and reduces the risk of unauthorized data access.

10. Install Mobile Security and Antivirus Applications

To further enhance security, users should install reputable mobile security and antivirus applications on their devices. These applications can detect and block malware, safeguard against phishing attempts, and provide real-time protection against threats. By maintaining up-to-date security software, users can ensure that their devices are constantly protected from evolving cyber threats.

By incorporating these 10 best practices into everyday IoT device management, users can significantly improve the security of their devices and mitigate risks. Implementing these measures not only safeguards individual privacy but also contributes to the overall security and reliability of IoT ecosystems.

Conclusion

In conclusion, the rise of Internet of Things (IoT) devices has highlighted the importance of mobile operating system security. Android, iOS, Windows, and Blackberry, while offering diverse functionalities, have been shown to be susceptible to various threats, including malware, data breaches, and unauthorized access. To address these challenges, a multi-faceted approach is necessary, involving robust security frameworks, continuous updates, user education, and collaboration between stakeholders.

Manufacturers can enhance IoT device security by prioritizing security from the outset of design and development, conducting regular security audits, and implementing strong access controls. As for users, they can contribute to a more secure IoT framework by being mindful of their online activities, avoiding suspicious links and downloads, and keeping their devices and software up to date. A collaborative effort between manufacturers, developers, users, and policymakers is essential to secure the future of IoT. By working together, we can build a more secure and resilient digital landscape where IoT devices can thrive without compromising our privacy or safety.

When choosing a mobile operating system for IoT devices, it is essential to evaluate the security features, compatibility, and user requirements. While each operating system, such as Android or iOS, offers distinct advantages, the decision should ultimately depend on factors like update frequency, security protocols, and the specific use case for the IoT device. A system that prioritizes regular security patches, encryption, and strong authentication methods is vital for protecting sensitive data and ensuring the overall safety of the IoT ecosystem. By considering these aspects, users can make an informed choice that best meets their security and functional needs without compromising the integrity of their IoT setup.

Works Cited

Adekotujo, A., Odumabo, A., Adedokun, A., & Aiyeniko, O. (2020, July). *A Comparative Study of Operating Systems: Case of Windows, UNIX, Linux, Mac, Android, and iOS*. https://www.researchgate.net/profile/Adedoyin-Odumabo/publication/372400705_A_Comparative_Study_of_Operating_Systems_Case_of_Windows_UNIX_Linux_Mac_Android_and_iOS/links/64b41d62c41fb852dd7b65e1/A-Comparative-Study-of-Operating-Systems-Case-of-Windows-UNIX-Linux-Mac-Android-and-iOS.pdf

Ahvanooey, M., Li, Q., Rabbani, M., & Rajput, A. (2017, October). *Malware attacks on smartphone OSes.* researchgate.net. https://www.researchgate.net/figure/Malware-attacks-on-smartphone-OSes_fig5_320734516

Ahvanooey, M., Li, Q., Rabbani, M., & Rajput, A. (2017, October). *Number of internet users (millions)*. Researchgate. https://www.researchgate.net/figure/Number-of-internet-users-millions-10_fig2_338853555

Ahvanooey, M. Prof. Q. L., Mahdi Rabbani, Ahmed Raza Rajput, Li, Q. M. R., Ahmed Raza Rajput, Rabbani, M., & Rajput, A. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *8*(10). https://arxiv.org/pdf/2001.09406

Aljaidi, M., Alsarhan, A., Samara, G., Alazaidah, R., Almatarneh, S. M. K., & Khalid, M. (2022, November 6). *NHS WannaCry Ransomware Attack: Technical explanation of the vulnerability, exploitation, and countermeasures*. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/10050485

Arthur, C., & Baxter-Reynolds, M. (2011, October 14). BlackBerry outage for three days caused by faulty router says former RIM staffer. *The Guardian*. https://www.theguardian.com/technology/2011/oct/14/blackberry-outage-faulty-router-suspected

La Polla, M., Martinelli, F., & Sgandurra, D. (2013, January 1). *A survey on security for mobile devices*. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/6170530

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019, October 1). *IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices*. IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8796409

Mohamed, I., & Patel, D. (2015, April 1). *Android vs iOS Security: A Comparative Study*. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/7113562

Weichbroth, P., & Łysik, Ł. (2020). Mobile security: threats and best practices. *Mobile Information Systems*, *2020*, 1–15. https://doi.org/10.1155/2020/8828078

Xiao, C. (2015, September 18). Malware XCodeGhost infects 39 iOS apps, including WeChat, affecting hundreds of millions of users. *Unit 42*. https://unit42.paloaltonetworks.com/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/