JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Android Malware Detection and Prevention

[1] Omkar Gawas, [2]Asst. Prof. Sonal Patil

[1,2]Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East)

Abstract: As Android smartphones continue to dominate the global market, they have become increasingly vulnerable to a wide range of security threats. This paper explores the factors contributing to the growing vulnerabilities in Android devices, including its open-source nature, ecosystem fragmentation, delayed security updates, and the proliferation of unregulated third-party app stores. Key threats such as malware, ransomware, phishing, and permissions abuse are examined, alongside emerging risks like cryptojacking, Advanced Persistent Threats (APTs), and the integration of Android with the Internet of Things (IoT). The paper also discusses the efforts by Google and the cybersecurity community to enhance Android security through initiatives like Google Play Protect, Project Treble, biometric authentication, and improved app vetting. Despite these advancements, challenges remain, particularly with the slow adoption of security patches and user awareness. The study concludes with recommendations for further improving Android security and emphasizes the need for ongoing collaboration between developers, manufacturers, and users to address the evolving threat landscape.

Keywords:- Android, Smartphone, Vulnerable, open-source, Malware, Security.

I. INTRODUCTION

In recent years, Android smartphones have experienced explosive growth in both popularity and functionality. This rise has made Android the dominant operating system in the smartphone market, holding a significant portion of the global user base. As of 2023, over 70percent of smartphones worldwide run on the Android operating system. Despite its widespread usage and open-source nature, Android has increasingly become vulnerable to various security threats, raising concerns among users, developers, and cybersecurity experts. This paper explores the reasons behind the growing vulnerabilities in Android devices, the evolving nature of the threats, and the efforts being made to mitigate these risks.

Open-Source Nature of Android: Android, developed by Google, is an open-source platform based on the Linux kernel. This openness has been one of Android's core strengths, allowing developers and manufacturers to customize the operating system to suit their specific needs. While this flexibility has driven Android's success, it also presents certain risks. The open-source nature of Android allows malicious actors to study the operating system's code, identify vulnerabilities, and exploit them. The Android ecosystem consists of numerous manufacturers, such as Samsung, Huawei, and Google itself, each modifying the Android operating system to create their own versions. This fragmentation results in inconsistent security patches and updates, leading to a wide range of Android versions being in use simultaneously. As a result, a significant portion of Android devices may remain unpatched and vulnerable to known security flaws.

Market Share and Popularity: Android's large market share makes it an attractive target for cybercriminals. The sheer number of Android devices in circulation increases the potential for exploitation. According to Statista, by the end of 2022, there were over 2.7 billion Android users globally. This massive user base has made Android a primary target for malware developers, hackers, and other malicious entities. The popularity of Android also means that any vulnerabilities discovered have the potential to impact millions of users, amplifying the consequences of a successful attack. Android Vulnerabilities is growing concern the increasing vulnerabilities in Android devices can be attributed to several factors, including the rise of sophisticated malware, delays in security patches, and the proliferation of unregulated third-party app stores. These vulnerabilities expose users to privacy breaches, data theft, financial loss, and even remote control of their devices.

Malware and Ransomware Attacks: Malware has become a significant threat to Android users, with cybercriminals continuously evolving their tactics to bypass security measures. Android's open nature allows users to download apps from various sources, including third-party app stores, which are often not regulated or vetted for malicious software. As a result, users may inadvertently install apps containing malware or ransomware. Ransomware attacks, in particular, have surged in recent years. Ransomware is a type of malware that encrypts a user's data and demands payment, often in cryptocurrency, to restore access. One high-profile case was the "Double Locker" ransomware, which targeted Android devices in 2017. This malware encrypted user files and locked the device's screen, demanding a ransom to unlock both. Such attacks have become more sophisticated, with some ransomware now capable of spreading across networks and encrypting data on multiple devices.

Phishing and Social Engineering: Phishing attacks are another common method used by cybercriminals to exploit Android vulnerabilities. Phishing typically involves tricking users into providing sensitive information, such as login credentials or financial

details, by masquerading as legitimate entities. These attacks can take the form of emails, SMS messages, or even fake mobile apps designed to mimic popular services. The rise of social engineering tactics has made phishing attacks more convincing and harder to detect. Attackers often tailor their messages to specific users, making them appear legitimate and trustworthy. For example, attackers may send fake notifications from banks or social media platforms, prompting users to click on malicious links or provide sensitive information. Once the attackers gain access to a user's account, they can steal personal data, commit identity theft, or initiate fraudulent transactions.

Delayed Security Updates and Patch Fragmentation: One of the major challenges in securing Android devices is the delayed rollout of security patches. While Google regularly releases security updates for the Android operating system, the responsibility for distributing these patches to user's falls on individual manufacturers and carriers. This results in significant delays in patching vulnerabilities, especially for older devices or devices from lesser-known manufacturers. Fragmentation in the Android ecosystem exacerbates this problem. Different manufacturers use different versions of Android, often modifying the system to suit their hardware. This customization process can delay the implementation of security updates, leaving devices exposed to known vulnerabilities for extended periods. In contrast, Apple's iOS, which has a more centralized update system, tends to patch vulnerabilities more quickly and efficiently.

App Store Security and Permissions Abuse: While Google Play Store has security measures in place to vet applications, malicious apps still manage to bypass these controls. Cybercriminals often use techniques such as code obfuscation, which makes it harder for automated systems to detect malicious behavior. Once these apps are installed, they can access sensitive data, track user activity, and even take control of the device. Permissions abuse is another issue in the Android ecosystem. Many apps request permissions that are unnecessary for their functionality, such as access to contacts, camera, or location data. Users often grant these permissions without fully understanding the implications, which can lead to privacy breaches and unauthorized data collection. This misuse of permissions has been a longstanding issue, and although Android has introduced measures to give users more control over permissions, many users remain unaware of the risks.

IoT and Android Integration: The growing integration of Android devices with the Internet of Things (IoT) has introduced new vulnerabilities. As smart devices become more prevalent in homes and businesses, many of these devices are controlled or monitored via Android smartphones. However, the security of IoT devices is often overlooked, and many IoT devices lack robust security measures. Cybercriminals have increasingly targeted IoT devices due to their often weak security protocols. Once an IoT device is compromised, it can serve as a gateway to other devices connected to the same network, including Android smartphones. This creates a broader attack surface, with the potential for large-scale data breaches, device hijacking, and denial-of-service attacks.

Evolving Threat Landscape the Android ecosystem faces a constantly evolving threat landscape. As security measures improve, cybercriminals develop new techniques to exploit emerging vulnerabilities. Some of the key trends in the evolving threat landscape include:

Advanced Persistent Threats (APTs): Advanced Persistent Threats (APTs) are highly targeted and sophisticated attacks often carried out by state-sponsored groups or well-funded criminal organizations. These attacks are designed to remain undetected for extended periods, allowing attackers to gather intelligence, steal data, or disrupt critical infrastructure. In recent years, APTs targeting Android devices have become more prevalent. For instance, the "Pegasus" spyware, developed by the Israeli cyber-intelligence firm NSO Group, was used to exploit vulnerabilities in both Android and iOS devices. Pegasus allowed attackers to remotely monitor and control infected devices, giving them access to messages, calls, and location data.

Cryptojacking: Cryptojacking is a form of cyberattack where attackers hijack a device's processing power to mine crypto currency. This type of attack has gained popularity with the rise of crypto currencies like Bitcoin and Ethereum. Crypto jacking can significantly degrade a device's performance, reduce battery life, and increase data usage. Android devices are particularly vulnerable to crypto jacking due to their widespread use and relatively lower processing power compared to desktop computers. Attackers often distribute crypto jacking malware through malicious apps or by exploiting vulnerabilities in web browsers.

5G and Network Vulnerabilities: The rollout of 5G technology promises faster internet speeds and more reliable connections. However, it also introduces new security challenges. As more Android devices connect to 5G networks, the potential for network-based attacks increases. 5G's increased bandwidth and lower latency make it easier for attackers to launch distributed denial-of-service (DDoS) attacks, where multiple devices are used to overwhelm a target system with traffic. Additionally, 5G networks rely on more complex infrastructure, including software-defined networking (SDN) and network function virtualization (NFV). These technologies, while improving network efficiency, also introduce new vulnerabilities that could be exploited by attackers to disrupt services or intercept data.

Efforts to Improve Android Security to address the growing vulnerabilities in Android devices, several initiatives have been implemented by both Google and the broader cybersecurity community. These efforts aim to enhance the security of the Android operating system and protect users from emerging threats.

Google Play Protect: Google Play Protect is a security feature introduced by Google to safeguard Android devices from malicious apps. It continuously scans apps installed on the device, as well as apps available on the Google Play Store, to detect and remove potentially harmful software. Play Protect also uses machine learning to identify suspicious behavior in apps and flag them for further analysis. While Play Protect has improved the security of the Google Play Store, it is not foolproof. Malicious apps can still bypass detection, and users who download apps from third-party sources remain at risk. Therefore, it is essential for users to exercise caution and only download apps from trusted sources.

Security Updates and Project Treble: In an effort to reduce fragmentation and accelerate the delivery of security updates, Google introduced Project Treble in 2017. Project Treble separates the Android operating system from the vendor-specific customizations

made by manufacturers. This modular approach allows Google to push security updates directly to devices without relying on manufacturers to implement the changes. While Project Treble has helped improve the speed of security updates for newer devices, older devices and those from smaller manufacturers still face delays in receiving critical patches.

User Awareness and Education: One of the most effective ways to reduce Android vulnerabilities is through user awareness and education. Many users are unaware of the risks posed by malware, phishing attacks, and permissions abuse, which leaves them vulnerable to exploitation. To address this, Google and cybersecurity organizations have invested in public awareness campaigns to educate users about best practices for mobile security. For instance, Google has introduced several features in Android, such as more granular app permission controls, which allow users to better manage what data an app can access. Additionally, warnings and prompts about potentially harmful behaviors—such as downloading apps from unknown sources—have become more prominent. Moreover, it is crucial for users to stay informed about the latest security threats and to develop habits that minimize their exposure to risks. This includes regularly updating software, being cautious about granting app permissions, and avoiding clicking on suspicious links in emails or text messages.

II. RESEARCH METHODOLOGY

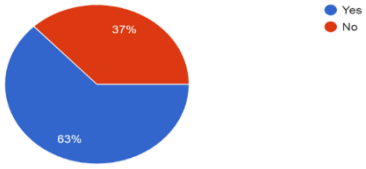
Hybrid model is an Examples may include descriptive and analytical content. Descriptive models can examine the relationship between relationships and conclusions drawn for the system's reasoning. But the results of the analysis actually differ from the chemical studies of substances in the body. We first surveyed people using an online survey and data collection service to learn about people's experiences.

III. PUBLIC SURVEY: QUESTIONNAIRE:

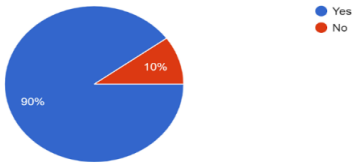
1. Do you regularly update your Android device's operating system?
2. Do you download apps only from official stores like Google Play?
3. Have you ever encountered a malware attack on your Android device?
4. Do you use antivirus or security apps on your Android device?
5. Do you enable Google Play Protect on your Android phone?
6. Have you ever granted unnecessary permissions to an app (e.g., access to contacts, camera, etc.)?
7. Do you regularly back up data on your Android device to prevent data loss from malware attacks?
8. Have you ever clicked on suspicious links or downloaded files from unknown sources?
9. Are you aware of the risks of downloading APK files from third-party websites?
10. Do you check app reviews and ratings before installing an app on your Android phone?

RESULT:

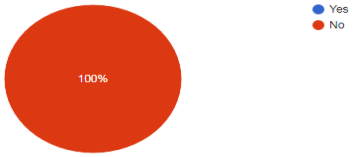
1) When we asked people "Do you regularly update your Android Phones operating system?" 63% people said yes and 37% people said no.



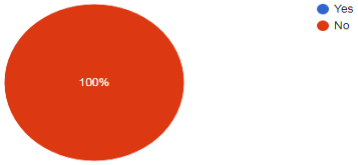
2) When we asked people "Do you download apps only from official stores like Google Play?" 90% people said yes and 10% people said no.



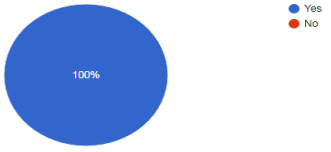
3) When we asked people do you think "Have you ever encountered a malware attack on your Android device?" 0% people said yes and 100% people said no.



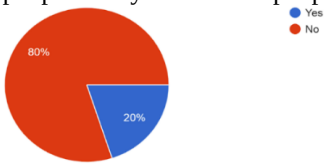
4) When we asked people do you think "Do you use antivirus or security apps on your Android device?" 0% people said yes and 100% people said no.



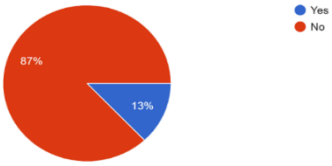
5) When we asked people "Do you enable Google Play Protect on your Android phone?" 100% people said yes and 0% people said no.



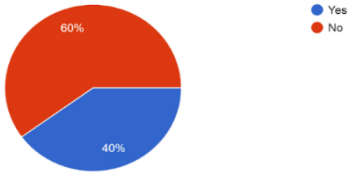
6) When we asked people "Have you ever granted unnecessary permissions to an app (e.g., access to contacts, camera, etc.)?" 20% people said yes and 80% people said no.



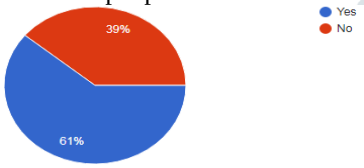
7) When we asked people "Do you regularly back up data on your Android device to prevent data loss from malware attacks?" 13% people said yes and 87% people said no.



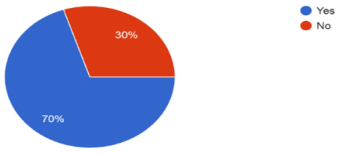
8) When we asked people "Have you ever clicked on suspicious links or downloaded files from unknown sources?" 63% people said yes and 37% people said no.



9) When we asked people "Are you aware of the risks of downloading APK files from third-party websites?" 61% people said yes and 39% people said no.



10) When we asked people "Do you check app reviews and ratings before installing an app on your Android phone?" 70% people said yes and 30% people said no.



IV. HYPOTHESIS TESTING

Hypothesis testing is a kind of statistical reasoning that includes analyzing data from a sample to originate implications about a population parameter or probability distribution. First, a hypothesis is created concerning the parameter or distribution. This is known as the null hypothesis, shortened as H0. After that, another hypothesis (denoted Ha) is defined which is the polar conflicting of the null hypothesis. Using sample data, the hypothesis testing method determines whether or not H0 may be rejected. The statistical conclusion is that the other hypothesis Ha is true if H0 is rejected.

For this paper:

Null hypothesis (H0): Malware is not the potential Threat to Android Phones.

Alternative hypothesis (Ha): Malware is truly the biggest Problem to android Phones and need to fix it.

1. Chi-squared test
2. T-student test (T-test)
3. Fisher's Z test

We will use 2 tailed t-test.

A t-test is an inferential statistic that controls if there is an important difference in the means of two collections that are related in some manner.

Level of significance a significance level of 0.05, for example, means there's a 5% probability of discovering a difference when there isn't one. Low significance levels indicate that more indication is required to reject the null hypothesis.

Level of confidence the confidence level indicates the probability that the location of a statistical parameter measured in a sample survey is also true for the entire population.

SR. No	Data
1	63
2	90
3	0
4	0
5	100
6	20
7	13
8	63

9	61
10	70
Mean(x)	**48**
Standard Deviation (s)	**4.37**

Level of significance = 0.05 i.e. 5% Level of confidence = 95%
The chances of rejecting the null hypothesis whether is true the significance level.
A t-score (t-value) is the number of normal deviations away from the t-mean distributions.
The formula to find t-score is: $t = (x- \mu) / (s/ \sqrt{} n)$
When x is the sample mean, μ is the hypothesis mean, s is the sample standard deviation, and n is the example size. The p-value, also known as the probability value, indicates how probably your data is to have happened under the null hypothesis. Once we know the value of t, we can find the corresponding p-value. If the p-value is less than alpha level (choices are .01, .05, and .10) then we can reject null hypothesis and accomplish that
Calculating t-value:
Step 1: Determine what the null and alternative hypotheses are.
Null hypothesis (H0): Malware is not the potential Threat to Android Phones.
Alternative hypothesis (Ha): Malware is truly the biggest Problem to android Phones and need to fix it.
Step 2: Find the test statistic.
In this case, the hypothesized mean value is consider 0.
$t = (x- \mu) / (s/ \sqrt{} n) = (78-0) / (4.37 / \sqrt{} 10)$
T-value = 56.44
Calculating p-value:
Step 3: Calculate the test statistic's p-value.
The t-Distribution with n-1 degrees of liberty is used to analyze the p-value. In this paper, the sample size is n =10, so n-1 = 9.
By working the observe value in the calculator, it returns a p-value. In this case, the p-value returned is less than 0.00001. Then this p-value is less than chosen alpha level of 0.05, we can reject the null hypothesis. Thus, we have sufficient evidence to say that Malware is truly the biggest Problem to Android Phones and need to fix it.

V. FINDINGS

1. As malware becomes more sophisticated, the role of machine learning in malware detection will become even more critical. Future research should focus on creating more advanced machine learning models that can adapt in real time to evolving malware patterns. These models could integrate more contextual data, such as network traffic analysis and user behaviour, to provide a more holistic view of potential threats.
2. User Education and Awareness Despite technical advancements in malware detection, user behaviour remains a significant factor in malware prevention. Educating users about the risks of installing apps from unknown sources, granting unnecessary permissions, and clicking on suspicious links can significantly reduce the likelihood of infection. Public awareness campaigns and in-device notifications could be used to reinforce these messages.
3. Hardware-assisted malware detection, such as Trusted Execution Environments (TEE) or TEE, can significantly enhance Android's security framework. A TEE is a secure area of the device's main processor that isolates and protects sensitive operations from the rest of the system.
4. Although Google Play Protect scans apps within the Play Store, third-party app stores and side loading remain significant vulnerabilities. Strengthening vetting procedures for these third-party apps through collaborations with trusted app store providers could mitigate the risks posed by non-official platforms. Implementing a standardized verification process for apps, similar to that used by Apple's App Store, would reduce the spread of malware through third-party channels.
5. One of the most persistent challenges in Android's security landscape is the slow rollout of security updates. Project Treble and Project Mainline (introduced in Android 10) have made progress in modularizing the Android OS and separating security updates from device-specific customizations.
6. The decentralized nature of block chain technology offers potential in securing app distribution. By leveraging block chain, app stores could create a transparent and immutable ledger of app metadata, ensuring that apps cannot be tampered with after being published.

VI. CONCLUSION

Android phones have become more efficient at protecting users from malware through a combination of advanced security frameworks, machine learning-based detection methods, and user control mechanisms. Google Play Protect, sandboxing, runtime permissions, and regular security patches all contribute to the overall resilience of the Android ecosystem. However, the open nature of the platform, combined with the fragmented device landscape and increasingly sophisticated malware, poses ongoing challenges. To maintain and improve the security of Android devices, several areas need continued focus, including reducing fragmentation, improving the consistency and speed of security updates, enhancing user education, and advancing machine learning-based detection methods. Hardware-based security solutions and the potential integration of block chain technology offer additional avenues for strengthening Android's defenses against malware. While Android's security architecture is robust and continually evolving, the threat landscape remains dynamic, requiring constant innovation and vigilance. With continued improvements in detection and prevention mechanisms, Android can further enhance its efficiency in protecting users from both known and emerging malware threats.

VII. REFERENCES

[1]Androguard. Static analysis tool for Android applications. Available at: https://androguard.readthedocs.io/.
[2]DroidBox. Dynamic analysis tool for Android applications. Available at: https://www.honeynet.org/project/Droidbox.

[3]Enck, W., Gilbert, P., Han, S., Tendulkar, V., others. TaintDroid: An information-flow tracking system for real-time privacy monitoring on smartphones. In Proceedings of OSDI 2010.
[4]Demontis, A., Melis, M., Biggio, B., Maiorca, D., others. Yes, machine learning can be more se- cure! A case study on Android malware detection. In IEEE Transactions on Dependable and Secure Computing, 2020.
[5]Sandeep Kumar, S., Sharma, S., & Saxena, A. Blockchain-based app store system: A next-generation malware detection and prevention system. In International Journal of Emerging Trends in Engineering Research, 2021.