Mobile Security: Threats, Defences, and Best Practices

By Keagan Robinson

***Abstract*—Mobile phones are an integral part of our daily life, however, their portability and connectivity make them vulnerable to cybercriminals as prime targets. This paper examines malware, phishing, network-based threats, and data leakage as the main focus of the security issues faced by mobile devices. Current defensive solutions such as multi-layered security protocols, mobile device management, and advanced authentication methods are also evaluated. In addition to this, research and industry insights, as well as emerging trends like artificial intelligence for threat detection and the challenges of 5G and Internet of Things (IoT) integration will be evaluated. The findings emphasise that organisations, and app developers need to collaborate to enhance mobile security.**

***Keywords*—Mobile security, malware, phishing, network-based threats, data leakage, authentication, mobile device management (MDM), biometric security.**

I. INTRODUCTION

A. Background

Mobile devices play a very important role in modern day-today life and are heavily used for communication, business, online shopping, and personal productivity. Excessive use and dependency on these devices leave them vulnerable to phishing attacks, malware, and network-based attacks. Recent studies show that over 60% of all cyberattacks are now primarily on mobile devices, and with increasing connections to the IoT, the push to secure these vulnerabilities is more pronounced than ever [5], [7]. The use of emerging technologies such as 5G and mobile devices within sensitive environments, such as healthcare and finance, broadens the potential attack vector for cybercriminals and multiplies the consequences of successful cyberattacks that may lead to device compromise and data breaches.

Ensuring cybersecurity in the mobile environment is much more complex than in traditional IT systems, with many more entry points for an attacker to potentially exploit. Short mobile development cycles and a lack of understanding of secure coding practices likewise offer opportunities for compromises. These attacks, however, are not infallible. Once the vulnerabilities of the mobile environment are understood, along with the most successful attack vectors and their causes, it becomes possible to develop a robust cybersecurity posture that not only protects mobile environments but also safeguards user privacy and ensures data integrity.

B. Scope and Objectives

This paper delivers a thorough summary of mobile security and focuses on the current most pressing aspects. This review centres around three key areas: the most prevalent threats to mobile security, the current available defences against those threats, and best practices for end users. This paper aims to achieve the following objectives:

- To identify the key security concerns that mobile devices face, including upcoming threats.
- To examine and assess current security frameworks and solutions, including multi-factor authentication, encryption, and Mobile Device Management (MDM) [2], [6].
- To make useful recommendations to improve mobile security procedures for people, businesses, and developers [3], [19].

This research highlights the importance of having a multilayered security strategy and working together with different groups, such as end-users, businesses, and policymakers, to build a strong mobile ecosystem that can handle changing threats [8], [12].

II. MOBILE SECURITY THREATS

A. Malware and Viruses

Mobile security is threatened by malware and viruses that target operating systems and applications. These malicious programs find their way into devices through app stores, phishing links, and compromised websites. For example, Android devices are frequently targeted because their open ecosystem allows harmful apps to pose as legitimate ones [5]. There are many types of malware, including spyware, which secretly watches what users do; ransomware, which holds users' devices hostage until a ransom is paid; and Trojans, which pretend to be safe programs while actually performing harmful functions. A well-known case is that of the Joker malware, which exploited its way into many Google Play Store apps, subscribing users to premium services without their knowledge [1],[3]. Malware is becoming more complex and polymorphic techniques to avoid detection, make the need for robust defences more pressing than ever. This means vetting apps and keeping software up to date [4].

B. Phishing and Social Engineering

Phishing is the act of sending an email with malicious intent with the aim of coercing recipients into disclosing information,

downloading malicious files, or completing actions they wouldn't normally do. Phishing in mobile contexts is similar to what happens on desktops or laptops, but it is often more personalised and therefore even more dangerous. This is because attackers can use different platforms to gather a lot of information about a person. From there, they can use tactics that are tailored specifically to overcome that person's unique vulnerabilities. A good example of this is the WhatsApp scam that attempted to steal the information of a global audience of users, leading many of them to download spyware onto their phones. It is very important to alert and instruct users in how to recognise phishing attempts. One way to accomplish this is to simulate internal phishing campaigns. By doing so, a business can identify its most vulnerable users before any potential threat actors can [11].

C. Network-Based Threats

Mobile devices are under serious threat from network-based attacks, especially when they connect to open public Wi-Fi networks. This is when an attacker in a Man-In-The-Middle (MITM) position can easily eavesdrop on the communications taking place between the mobile device and the network. By posing as a legitimate Wi-Fi hotspot, an attacker can use a rogue access point to pull unsuspecting users off the legitimate network and onto a fake network. Once a user is on the fake network, the attacker can see everything that the user is doing and effectively harvest any unencrypted or easily decrypted data [12].

Mobile devices also face the threat of Denial-of-Service (DoS) attacks. DoS attacks affect the mobile device more than the network because they are by nature resource-intensive for the attacking device and the deceptive elements in the network. The dangers are heightened in the context of 5G networks, which, while offering improved speed and connectivity, also provide new opportunities for attackers due to their distributed architecture [13]. One of the most effective high-tech countermeasures to these threats involves the use of Virtual Private Networks (VPNs) and the activation of encrypted communication protocols [14].

D. Device Theft and Unauthorised Access

Mobile devices are inherently portable, making them attractive targets for thieves and presenting a considerable security risk to users. When a device is stolen, there is the immediate risk of unauthorised access, which can result in a data intrusion, especially if the device was not well secured [8]. Some of the best practices for securing a mobile device also serve as common sense and are reminiscent of keeping a regular computer secure. They encompass good password hygiene, the use of screen lock functions, and enforcement of encryption policies. Mobile device monitoring applications that may come with a device, including "Find My Device," also serve as an important way to secure data in the event that a device is not merely lost but stolen [9].

E. Privacy Invasion and Data Leakage

User data are collected in vast amounts and in many different forms within mobile applications and services, often far exceeding what is needed for the apps' operational purposes. This excessive and often unauthorised collection of data, which can even include the tracking of users' locations and access to their contact lists, has caused real and potential privacy violations, not to mention the possibility of significant data breaches [19].

Apps lacking adequate security can reveal private information during transmission or while stored, making them vulnerable to breaches. A prime example of this is the scandal involving Facebook and Cambridge Analytica. Inadequate data governance allowed the unauthorised gathering of millions of users' data [22]. This incident now stands as a sobering testament to the potential consequences associated with poor app security. Breaches can happen, and they do not have to be sophisticated to be damaging. In addition to this, there is a growing issue of adware that collects user data to serve users with more targeted ads, taking away from privacy.

Mandatory regulations such as the General Data Protection Regulation (GDPR) are making a push to control these practices by establishing firm data protection demands. They have, if nothing else, gotten people talking about the importance of being in good control of what kinds of data are shared with apps and about being really aware of the kinds of data that might be in danger of being shared [21].

III. DEFENSIVE STRATEGIES IN MOBILE SECURITY

A. Operating System Security Mechanisms

The mobile security of an operating system depends significantly on its security architecture, which encompasses both the built-in features of the OS and its access control mechanisms. In both big-name platforms, Android and iOS, applications are isolated from one another and from the OS itself, which is a core aspect of the sandboxing security model [5]. In Apple's iOS, a closed-source system, user access to systemlevel functions is highly restricted, thus reducing potential attack vectors. On the other hand, Android is built on top of Security-Enhanced Linux, or SELinux, which provides mandatory access controls that, in effect, harden the open ecosystem surrounding Android [15]. Applications and system resources remain secure, with virtual boundaries that prevent unauthorised access. Both operating systems have had vulnerabilities discovered in them, but Apple's iOS has a much better track record in this area. Full-disk encryption, which was introduced in iOS 8 and in Android 5.0, is another layer of built-in security that is now present on most modern mobile devices [13].

B. Application Security Practices

The security of mobile applications is dependent upon secure coding practices and regular vulnerability assessments. Developers must follow secure coding guidelines, such as those offered in the Open Web Application Security Project (OWASP) Mobile Security Testing Guide. These guidelines and the tools and techniques associated with them minimise coding errors that create vulnerabilities [23]. The direct application of obfuscation and hardening techniques also makes

the app more secure, deterring reverse engineering and tampering. Regular assessments, both static and dynamic, identify any remaining vulnerabilities before deployment and allow the developer to fix them [6]. Even the app store that serves the apps plays a critical role in overall security. Google Play Protect, for instance, uses machine learning to scan billions of apps for malicious behaviour and ensures that the application ecosystem as a whole remains secure.

C. Network security approaches

Ensuring the safety of mobile network communications is essential. Yet when mobile devices connect to largely unsecured public Wi-Fi networks, the risk of interception rises. Wireless encryption protocols like WPA3 provide a pretty good first line of defence. But even the best wireless encryption can be defeated by a determined (and often well-funded) adversary.

Thus, using a VPN to create an added layer of encryption for the network communications of a mobile device is a very good idea, especially in environments with a heightened risk of interception. Protocols for secure communication, such as Transport Layer Security (TLS), safeguard sensitive data sent across networks [13]. For example, TLS often encrypts transactions for financial and e-commerce applications, thereby ensuring the confidentiality and integrity of the data being exchanged [14].

Organisations can also use Intrusion Detection and Prevention Systems (IDPS) to monitor and even shut down variants of malicious network traffic [15]. The decentralised architecture, increased capacity, and speed of 5G create a whole new set of potential attack surfaces that require the adoption of zero-trust network principles [16].

D. Authentication Methods

Mobile devices and the data within them are under constant threat. Protecting them with strong authentication is more critical than ever. The gold standard for the moment is multi-factor authentication, which depends on two or more credentials from the following three categories: something the user knows (like a password), something the user has (like a security token), and something the user is (like biometric data) [24]. For mobile phones, biometric authentication such as fingerprint scanning, facial recognition, and voice recognition has gained prominence and has become very reliable. Modern Apple and Android devices now offer advanced biometric authentication on their devices, with examples including fingerprint scanning, facial recognition, and voice recognition [9]. Biometric methods hold many advantages, yet they do not represent an infallible solution. Since physical biometric data can be spoofed and biometric systems can be physically coerced into granting access, these methods can be vulnerable to several types of attacks.

Public Key Infrastructure (PKI) and FIDO2 standards provide refined security in authentication. They, along with several other state-of-the-art methods, eliminate the reliance on passwords and offer greater convenience and security without the use of a password. Companies are encouraged to implement adaptive authentication, which dynamically adjusts security levels based on user behaviour and context.

E. Mobile device management (MDM)

MDM solutions are essential for managing and securing devices within organisations. These tools allow IT administrators to enforce security policies, monitor device usage, and remotely wipe lost or stolen devices. Features such as geofencing enable organisations to restrict device access based on location, enhancing physical security [25]. Examples of MDM solutions include Microsoft Intune and VMware Workspace ONE, which provide centralised platforms for managing device compliance and deploying security updates. Application control is another significant MDM feature, and it reduces exposure to malware by ensuring that only approved apps are installed on managed devices. In addition, integrating MDM with Endpoint Detection and Response (EDR) tools can significantly enhance an organisation's ability to detect and mitigate threats in real time.

However, implementing MDM may face employee resistance due to privacy concerns, so it is critical to balance security requirements with user autonomy. Integrating MDM with EDR tools improves an organisation's ability to detect and mitigate threats in real time.

IV. BEST PRACTICES FOR MOBILE SECURITY

A. Recommendations for Individual Users

Personal mobile security starts with the user taking safe actions and using available security mechanisms. Mobile users should keep their devices updated, ensuring that both the operating system and applications are current. Because delayed updates give attackers more time to weaponise newly discovered vulnerabilities, enabling automatic updates where possible is a good security practice. Keeping mobile devices secure also relies on using passwords and other access controls. Although some might argue that mobile devices have become so powerful that they deserve the same strong access controls as desktop computers, many mobile users seem to prefer the kind of speedy, frictionless access one gets with a less secure device.

App permissions should be carefully examined by users, who should only grant those that are necessary for the app to function. This scrutiny is necessary because too many permissions can lead to loss of data and invasions of privacy [5]. To avoid malicious applications, users should install apps only from trusted sources, such as official app stores [6]. Another way users can protect themselves is by using antivirus software that is designed for mobile devices. Such software can detect and stop malware from doing harm [7].

B. Organisational Policies

It is of utmost importance to have strong policies in place for securing mobile devices in corporate settings. Companies must implement Bring Your Own Device (BYOD) policies that strike a balance between allowing employees the freedom to use their personal devices and meeting the required security protocols. Organisations should provide clear guidelines about what is considered acceptable use of the device, what apps can be installed on the device, and how data can be shared when

using the device [26]. MDM tools are then used to enforce these policies [9] while allowing the audibility necessary to keep both the employer and the employee safe.

Training employees on a consistent basis creates a culture of security and is mandated by federal regulations for certain industries. Beyond this basic level of security, it is wise to implement several other layers of security in a corporate environment. One such layer is segmentation. Segmentation simply means dividing the network into parts, and it is a good idea for several reasons, most importantly that it restricts access to sensitive data and systems. By not allowing eavesdroppers to reach the data that is being encrypted, segmentation keeps both the employees and the systems that they are using secure. Corporate VPNs must be mandatory for remote workers accessing sensitive systems. These systems create secure communication channels, hinder cybercriminals, and keep data from being intercepted. That said, if a device is lost or stolen, the incident response plan must tell responders to treat the incident like a potential data breach because the device in question is an access point to the network and a storage point for potentially sensitive data.

C. Developer Guidelines

End-user security rests heavily on the shoulders of app developers. To bolster security, it is vital that developers engage in the secure coding practices of the past, as well as those of the present. These practices include, but are not limited to, input validation and output encoding to help avoid common vulnerabilities like injection attacks and Cross-Site Scripting (XSS). Hard-coded secrets are vulnerable, and developers should steer clear of this. When developers use frameworks and libraries to develop their apps, they should make use of those with built-in security features.

It is crucial to perform routine vulnerability assessments, including both static and dynamic analyses, to pinpoint security weaknesses before an app goes live [21]. Attack-simulation tools such as OWASP ZAP or Burp Suite can determine whether the app can stand up to actual attacks. Overall, maintaining user privacy should be of utmost importance. This goal can be accomplished by minimising the collection of data, securely encrypting all data whether it is in transit or at rest, and transparently informing users of what data is being collected and for what purpose. It is also very important for developers to follow secure distribution practices when they are launching their apps. They should be signing their apps with trusted certificates to ensure the apps are verified and authentic and should be following app store submission guidelines to reduce the risk of tampering with the apps. Once an app has been released, the developers must now maintain the app's security and integrity in light of new emerging threats and vulnerabilities that occur postlaunch.

V. EMERGING TRENDS AND FUTURE DIRECTIONS

A. Artificial Intelligence and Threat Detection

Mobile security is being transformed by artificial intelligence, which is enabling proactive threat detection and even mitigation, in some cases. Vast amounts of data can be analysed by machine learning algorithms to identify malicious activities. The anomalies found in these patterns tend to be the sorts of things that humans would miss, and even unusual app behaviour or network access could be detected by a nasty bit of work that a mobile security component may identify as a zeroday threat. In these situations, preemptive measures would be welcomed by any organisation that has a mobile workforce; and as the complexity of the mobile landscape only promises to deepen, it will take a good deal of teamwork among software developers, threat researchers, and other security professionals to ensure that AI does what it can do best in a mobile context and secure it.

B. Advances in Biometric Security

Authentication based on biometrics has made great strides, yielding not just more secure but also more user-friendly portals to a variety of mobile devices. One example of this is 3D facial recognition, like that used in Apple's Face ID. This technology employs a depth-sensing camera that determines the correct distance of the user's face from the device. This superior technology prevents "visual" hacks using photographs or even life-size silicone masks, which unfortunately work quite well with traditional front-facing cameras and the image processing that goes along with them. Similarly, we now have fingerprint readers that use ultrasonic sound waves instead of capacitors to "feel" the ridges and valleys in our fingerprints. These readers, like those in many modern Android devices, provide much more accurate and reliable access.

C. Implications of 5G and IoT

5G networks and IoT devices are fundamentally changing the mobile security landscape. They create new forms of interaction with users and new opportunities for cybercriminals to access sensitive information, which is why they represent both opportunities and challenges for mobile security architects. 5G allows for the seamless integration of the IoT ecosystem; its low latency and high-speed connectivity can truly supercharge the automation and productivity promised by IoT devices [27]. However, compromised IoT devices significantly raise the stakes for network security. In general, the IoT device ecosystem represents a new avenue for the hacking community because devices are often poorly secured. One notorious botnet attack, launched via an insecure network of IoT devices, took down much of the internet for a day.

These risks can be reduced only if the mobile security ecosystem adopts zero-trust principles, enforces strong IoT security standards, and collaborates across the industry, which will ensure the mobile environment's overall security posture. This goal demands an efficiently working assembly of developers, manufacturers, and regulators to address these pressing challenges.

VI. CONCLUSION

Mobile devices are crucial in modern society, enabling connectivity, business transactions, and productivity. However, they also pose security risks, impacting both online and offline

lives. Emerging technologies like AI, 5G networks, and IoT present opportunities but also introduce challenges. To ensure mobile security, organisations must involve stakeholders from the start, engaging them in dialogue and seeking their assistance. This involves fostering a secure organisational culture and involving service providers, application developers, and users. Mobile security is a collective responsibility, requiring active participation from all stakeholders. Engaging stakeholders in discussions about security can strengthen the mobile ecosystem and enhance system protection. Implementing these measures can help organisations maintain a secure online and offline existence.

REFERENCES

[1] D. He, S. Chan, and M. Guizani, "Mobile application security: Malware threats and defences," IEEE Wireless Communications, vol. 22, no. 1, pp. 138–144, February 2015, doi: 10.1109/MWC.2015.7054729.

[2] NIST, "Guidelines for managing the security of mobile devices in the enterprise," Special Publication 800-124 Revision 2, June 2020. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-124r2.

[3] S. V. Ilapakurthy, "Bolstering the mobile cloud: Addressing emerging threats and strengthening multi-layered defences for robust mobile security," 2023 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), San Antonio, TX, USA, 2023, pp. 1–7, doi: 10.1109/IOTSMS59855.2023.10325824.

[4] I. Ghafir, and V. Prenosil. "DNS query failure and algorithmically generated domain-flux detection." In International Conference on Frontiers of Communications, Networks and Applications, Malaysia, pp. 103-107, IET, 2014.

[5] U.S. Department of defence, "Mobile device best practices," July 2020. [Online]. Available: https://media.defence.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE DEVICE BEST PRACTICES FINAL V3%20-%20COPY.PDF. [Accessed: Nov. 22, 2024].

[6] P. Faruki, R. Bharmal, V. Laxmi, M. Gaur, and S. Rajarajan, "Android security: A survey of issues, malware penetration, and defences," IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 998–1022, Secondquarter 2015, doi: 10.1109/COMST.2014.2386139

[7] NIST, "Mobile device security: Bring your own device (BYOD)," Special Publication 1800-22, Sep. 2020. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.1800-22.

[8] S. Eltanani and I. Ghafir, "Coverage Optimisation for Aerial Wireless Networks," 2020 14th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, 2020, pp. 233-238, doi: 10.1109/IIT50501.2020.9299076.

[9] G. Helm and M. M. Chowdhury, "Security issues of mobile devices: A survey," 2021 IEEE International Conference on Electro Information Technology (EIT), Mt. Pleasant, MI, USA, 2021, pp. 014–020, doi: 10.1109/EIT51626.2021.9491840.

[10] NIST, "Guidelines for managing the security of mobile devices in the enterprise," Special Publication 800-124 Revision 1, Jun. 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-124r1.

[11] Abdulhamid, S. Kabir, I. Ghafir and C. Lei, "Dependability of the Internet of Things: Current Status and Challenges," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-6.

[12] S. Grzonkowski, A. Mosquera, L. Aouad, and D. Morss, "Smartphone security: An overview of emerging threats," IEEE Consumer Electronics Magazine, vol. 3, no. 4, pp. 40–44, Oct. 2014, doi:

[13] U.S. Department of defence, "Evaluation of Department of defence cybersecurity policies," Report No. DODIG-2023-041, Feb. 2023. [Online]. Available: https://media.defence.gov/2023/Feb/09/2003159280/1/-1/1/REVISED_DODIG-2023-041.PDF. [Accessed: Nov. 25, 2024].

[14] "Analysis of mobile threats and security vulnerabilities for mobile platforms and devices," in Security, Privacy and Reliability in Computer Communications and Networks, River Publishers, 2017, pp. 139–174.

[15] F. J. Aparicio-Navarro, T. A. Chadza, K. G. Kyriakopoulos, I. Ghafir, S. Lambotharan and B. AsSadhan, "Addressing Multi-Stage Attacks Using Expert Knowledge and Contextual Information," 2019 22nd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), Paris, France, 2019, pp. 188-194, doi: 10.1109/ICIN.2019.8685841.

[16] NIST, "Vetting the security of mobile applications," Special Publication 800-163 Revision 1, Apr. 2022. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-163r1.

[17] T. Zhao, G. Zhang, and L. Zhang, "An overview of mobile devices security issues and countermeasures," 2014 International Conference on Wireless Communication and Sensor Network, Wuhan, China, 2014, pp. 439–443, doi: 10.1109/WCSN.2014.95.

[18] U.S. Department of defence, "Identity and access management recommended best practices for administrators," Report No. PP-23-0248, Mar. 2023. [Online]. Available: https://media.defence.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED BEST _PRACTICES PP-23-0248.pdf. [Accessed: Nov. 27, 2024].

[19] Q. Li and G. Clark, "Mobile security: A look ahead," IEEE Security & Privacy, vol. 11, no. 1, pp. 78–81, Jan.–Feb. 2013, doi: 10.1109/MSP.2013.15.

[20] NIST, "Guidelines on mobile device forensics," Special Publication 800101 Revision 1, May 2014. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-101r1.

[21] M. Lefoane, I. Ghafir, S. Kabir and I. -U. Awan, "Multi-stage Attack Detection: Emerging Challenges for Wireless Networks," 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), Palapye, Botswana, 2022, pp. 01-05, doi: 10.1109/SmartNets55823.2022.9994027.

[22] A. Mos and M. M. Chowdhury, "Mobile security: A look into android," 2020 IEEE International Conference on Electro Information Technology (EIT), Chicago, IL, USA, 2020, pp. 638–642, doi: 10.1109/EIT48999.2020.9208339

[23] U.S. Department of defence, "CSI: Securing wireless devices in public," Jul. 2021. [Online]. Available: https://media.defence.gov/2021/Jul/29/2002815141/-1/-1/0/CSI SECURING WIRELESS DEVICES _ IN PUBLIC.PDF. [Accessed: Nov. 29, 2024].

[24] S. Eltanani and I. Ghafir, "Aerial Wireless Networks: Proposed Solution for Coverage Optimisation," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Vancouver, BC, Canada, 2021, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484609.

[25] NIST, "Zero trust architecture," Special Publication 800-207, Aug. 2020. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-207

[26] Y. Wang, C. Hahn, and K. Sutrave, "Mobile payment security, threats, and challenges," 2016 Second International Conference on Mobile and Secure Services (MobiSecServ), Gainesville, FL, USA, 2016, pp. 1–5, doi: 10.1109/MOBISECSERV.2016.7440226.

[27] NIST, "Managing information security risk: Organization, mission, and information system view," Special Publication 800-39, Mar. 2011. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-39.