Mobile Devices Technologies: Risks and Security

[1]Raed Alsaqour, [1]Sultan Alharthi, [1]Khalid Aldehaimi, [2*]Maha Abdelhaq
[1]Department of Information Technology, College of Computing and Informatics,
Saudi Electronic University, 93499 Riyadh, Saudi Arabia
[2]Department of Information Technology, College of Computer and Information Sciences,
Princess Nourah bint Abdulrahman University, 84428 Riyadh, Saudi Arabia
[1]{r.alsaqor@seu.edu.sa, s170013804@seu.edu.sa, s180004914@seu.edu.sa}
[2*]{Corresponding Author: msabdelhaq@pnu.edu.sa}

Abstract
Our society is depending on mobile devices that play a major role in our lives. Utilizing these devices is possible due to their speed power and efficiency in performing basic as well as sophisticated operations that can be found in traditional computers like desktop workstations. The challenge with using mobile devices is that organizations are concerned with the interference between personal and corporate use due to Bring Your Own Device (BYOD) trend. This paper highlights the importance of mobile devices in our daily tasks and the associated risks involved with using these devices. Several technologies and countermeasures are reviewed in this paper to secure the mobile devices from different attempts of attacks. It is important to mention that this paper focuses on technical measures rather than considering different aspects of security measures as recommended by the cybersecurity community.

Key words:
Mobile Security; BYOD; Multifactor Authentication; MDM; MSS; Security Policy.

1. Introduction

Mobile devices are playing vital roles in our lives [1]. These mobile devices include laptops, smartphones, Personal Digital Assistant (PDAs), and others. People nowadays utilizing these devices to perform both personal and professional tasks from anywhere and anytime [2]. Making this possibility is a huge risk to the organizations. It is difficult to enforce employees to keep their devices at home, while they prefer utilizing them to shorten the achievement time for the good of their firms. Bring Your Own Device (BYOD) trend allows employees to maximize productivity and flexibility in their firms [3]. Letting the government and private sectors considering the permission of using these devices for doing professional tasks. Some organizations attempted to use mobile devices for employees' attendance and monitoring the employee's activities during working hours [2]. Others allowed their employees to perform critical tasks on their mobile devices like scheduling meetings, file printing, document processing, and much more. With considering the personal use via these devices, mobile devices became essential in doing financial processes like transferring money via banking applications and doing online payments [4].

Manuscript received April 5, 2021
Manuscript revised April 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.4.30

With all that has been said, users and professionals agree on the importance of mobile devices for both personal and corporate uses. Therefore, the security of mobile devices is a must, due to their processing power and the sensitive data that might be contained in them by individuals [5, 6] Many factors have to be considered when putting in mind the security of mobile devices. They are, but are not limited to, the nature of the mobile devices, the vulnerabilities, and threats that are associated with every device, and the acceptable level of security used on these devices [5].

Some surveys have been released that 78% have sensitive data in their mobile devices [5]. However, only 62% of them used encryption, passwords, and PINs for protection. This raises the idea of the importance of training and warning of such risks. Another thing that overwhelms the normal users and organizations' representatives is the growing concern of mobile malware like viruses, worms, and trojan horses. These malware applications are not infecting desktop devices only. They infect all kinds of mobile appliances too [5].

The rest of this paper is organized as follows. In Section 2, we provide risks and issues in mobile devices. In Section 3, we present technologies to secure mobile devices. In Section 4, we describe general guidelines to secure mobile devices. Finally, the conclusion and possible directions for future work are in Section 5.

2. Risks and Issues in Mobile Devices

There are risks and issues accompanied with using mobile devices. These risks are due to the flexibility of mobile devices' usage. Also, mobile devices do not require the limitation of physical existence, they can do the required tasks from anywhere and anytime as long as there secure wireless connectivity [7]. These security risks are, but not limited to:

- *Wireless Interception*. Many public places offer free wireless connections. It is not guaranteed that these access points are secured completely. An

attacker can utilize these connections to perform Man-In-The-Middle (MITM) attack [8].

- *Probing.* This happens when an attacker directing certain traffic – usually intended for sensitive data – to the attacker's destination causing confidential data to be stolen [9].
- *Weak or Null Authentication*. Without proper and strong authentication, all sensitive resources will be easily compromised by unauthorized users [10].
- *Lacking Training and Awareness*. Unfortunately, many users are not aware of the existing vulnerabilities and threats associated with their data in their mobile devices. Attackers are intentionally targeting these naïve users using techniques and approaches like social engineering [11].

3. Technologies to Secure Mobile Devices

This section proposes several valuable technologies and recommendations to secure the mobile devices and thwart the attacker's initiatives in attempting to compromise mobile devices [12].

3.1 Multifactor Authentication

BYOD trend involves using mobile devices like smartphones. These smartphones come with hundreds or even thousands of applications for personal and professional needs. These devices made everyday life easy and productive. Smartphones can be used now as attendance appliances for example. Therefore, they must ensure that employees cannot make fraud in recording the attendance for themselves or sabotaging the attendance records for others [2].

Multifactor authentication can be utilized to secure mobile devices and their associated applications. There are three general authentication types; something you know, something you have, and something you are. Something you know like using a password. Something you have like a key or a token. And something you are like your fingerprint, retina scan, or your voice's patterns. While many firms use only one of the aforementioned factors and a single factor might be susceptible to intruders, having multiple authentication factors is recommended to secure any digital system, especially mobile devices. Secure IDs for android devices, GPS, fingerprints, and other factors can be combined to serve the purpose of securing the mobile devices, whether for personal or professional uses. The more authentication factors used; the better mobile security will be [2].

3.2 Domain Separation

Many organizations face the fact that they are enforced to let their employees use their mobile devices to perform the work's tasks efficiently. Smartphones, Laptops, Tablets, and others are utilized in work environments. Making them access the sensitive data and critical resources of their organizations anytime and anywhere. Therefore, security professionals have to consider such risks of letting the employees do their work without putting the effective measures to secure the digital resources [3].

The logical approach to let the employees do their tasks with their devices and not affecting the security of the organization's data is separating the personal domain – which is also called a normal domain in some sources – from the secure domain. That way the employees can perform both personal and professional tasks without risking interrupting the sensitive data. There is a solution called Mobile Device Management (MDM) that will be discussed later in this paper which serves the same purpose. However, many recommendations said that there are vulnerabilities and drawbacks in this solution, making it difficult to offer absolute security. Those vulnerabilities can allow attackers to install malicious software on mobile devices through MDM solutions [3].

Fortunately, a proposed solution that has been released recently called Mobile Security Solution (MSS) that offers strong security between the separated domains (Normal & Secure).

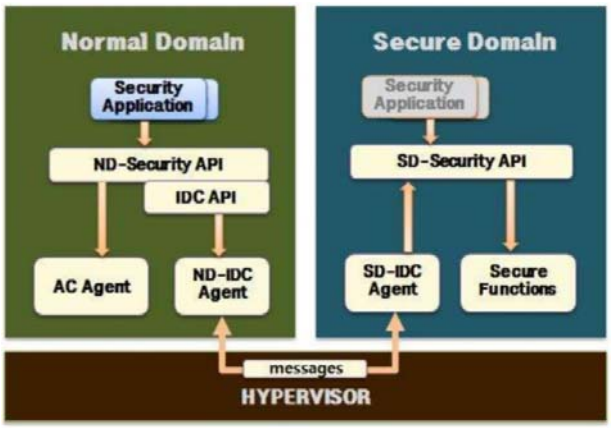

Fig. 1 MSS System Architecture

Fig. 1 shows how the MSS is working. MSS separates the two domains using a hypervisor that secures the domains completely. The secure domain – with the help of the hypervisor – can perform secure functions like data encryption and decryption, signature creation, and key storage in a well-isolated area without interfering with the normal (personal) domain. MSS can encrypt, decrypt

certificate files of the public key securely. MSS serves that purpose because it is based on the TEE system of a global platform. This system includes several components like – but not limited to – REE communication agent, TEE functional API, trusted core framework, trusted functions, and others. Both domains can be communicated through a secured channel using the built-in hypervisor. This technology can be used in securing mobile devices [3].

3.3 Mobile Payment Security

Mobile devices nowadays are helpful when it comes to online payment. Users must ensure the security of the transactions via their mobile devices. Thus, securing the mobile device itself [4].

There are alternative ways to perform digital transactions securely. This can be done by using J2ME-enabled mobile phones over Bluetooth. The major benefits gained from this technology are [4]:

a) Running the same contents with carriers utilizing a wide range of manufacturers.
b) The code used between devices is portable.
c) The technology provides safe and secure network delivery through the Internet.
d) Allowing more interactive applications with a full runtime environment.
e) And offline operation.

Those benefits are helping mobile devices to perform payment transactions securely. Implementing these components in a basic security solution of the payment system can give the system the following security features [4]:

a) *Account Service*: which gives the user an account before using the payment service in the Bluetooth environment.
b) *Access Control*: The authorization comes after the authentication. The user must provide additional indicators to make sure that he is the one who claimed the access in the first place.
c) *Security Verifications*: the user must provide a password that matches the previous one that was inserted in the database to access the account successfully.

All the previous tools are presented to offer a secure environment for payment using mobile devices. One can never ignore the importance of mobile device security in our daily lives.

3.4 Biotelemetry

Another technology that might be helpful when it comes to securing mobile devices is Biotelemetry. The idea suggests a Secure Mobile Computing (SMC) system that detects the individual's body signals. These signals are referred to as electrocardiograph (ECG). ECG waveform can differ from one person to another. The system can analyze those waves and determine the signal changes and respond to those patterns based on predefined policies [5].

The system monitors several parameters of the body like ECG, blood pressure, temperature, blood oxygenation, and respiration. ECG is critical for this matter because of two reasons; first, ECG reveals information about the individual's health. Second, ECG indicates other signals like respiration and blood pressure. These parameters help the mobile device's user to ensure the security of his/her device [5].

However, there are challenges associated with the balancing between usability and security within SMC. They are as follows:

a) The lifetime of the system must be reasonable.
b) SMC service should not overwhelm the device's performance.
c) The error rate should be low and doesn't affect the overall performance.

SMC system technology involves several contributions that serve the purpose of securing mobile devices:

a) A printed electronic circuit for sensing ECG signals containing three electrodes.
b) An algorithm for heart rate detection.
c) An application for users that have generic interfaces like sensor type, radio frequency (Fig. 2).
d) A simulator that models the design space of the system.
e) A web application service for the mobile device to communicate with the backend network.

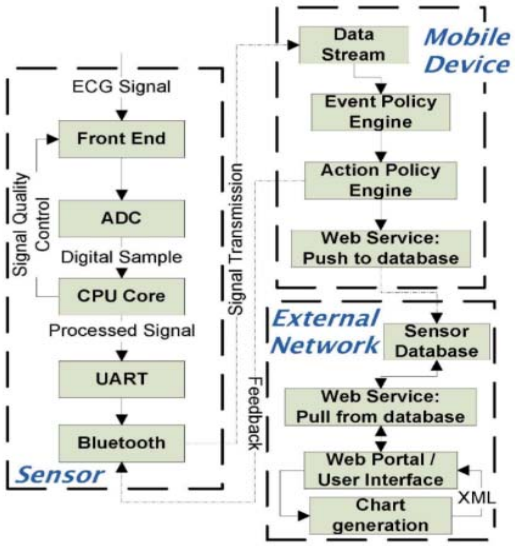

Fig.2 Sensor in Mobile Device

3.5 Mobile Device Management (MDM) System

One technology that serves mobile devices security, is having a system that manages mobile devices by monitoring the devices' activities and status as well as controlling the functions remotely via wireless communication like Wi-Fi technology. In addition, the system can manage the required business resources [13].

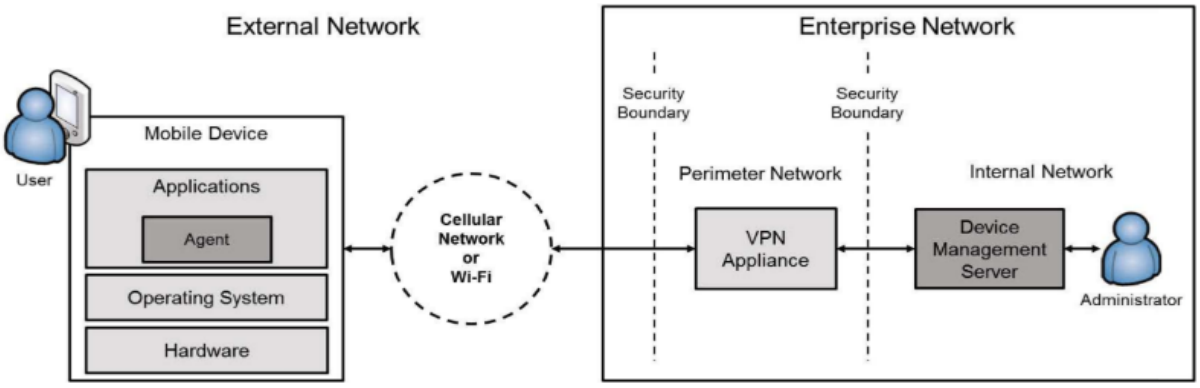

Fig. 3 Operational Environment of an MDM System

As shown in Fig. 3, the system consists of two parts: the mobile device's components and the enterprise network's components. The administrator takes control of the device management server via a web browser. The Agent in the mobile device serves as an application that is installed in the mobile device to collect different types of data and send them to the device management server. The Agent also applies the policies sent from the device management server and sends back the results to the device management server. The device management server manages the data received from mobile devices. Also, it distributes the policies to all agents in the operational environment. A Virtual Private Network (VPN) can be utilized in this system to connect between the two networks securely even though it is not necessary. VPNs can be replaced by other secured technologies like – but not limited to – IPSec, SSH, TLS/HTTPS, TLS, and cryptography techniques [7].

3.6 Securing the Mobile Applications

It is important to remember that to secure your mobile device, you have to consider securing every component associated with it. Mobile applications are essential parts of such devices. Like desktop devices, mobile devices are used by almost everyone to perform personal and professional tasks. Generally speaking, mobile devices are much risky than other devices that use wired connections. That is because mobile devices can move and work everywhere and anytime. In addition, people tend to be less careful of protecting these devices. This is a serious security issue that must be handled properly. The following section points out several measures considering securing mobile applications [13].

3.6.1 Configuring SSL

Secure Socket Layer (SSL) is a protocol used with the association of HTTP protocol to secure the connection between the web browser of the mobile device and the web server hosting the web pages. The connection – with the help of SSL – will be encrypted interfering with outsider attackers quite impossible [13].

3.6.2 Setting Timeout

Due to the use of BYOD trend nowadays, people who perform their tasks in the public area are quite obvious. Therefore, they might get distracted by other parties or their surroundings. Although this observation is common and cannot be denied, there is a simple, yet powerful, a step that can be taken to lower the risk of taking control of mobile devices without the notice of the original owner. Applications can be timed out using a feature that almost all operating systems are having it. The user can set a timer of one minute, for example, if he leaves for urgent reasons, it is harder for intruders to take control of the device and do malicious behaviors or at least steal valuable information. As shown in Fig. 4, the user can set a timer, and once the timer finishes, he/she can direct the session to a specific URL or the main login page [13].

Fig. 4. Login Page After the Timeout is Finished

3.6.3 Data Encryption

Previously, the paper mentioned SSL and HTTPS protocols to encrypt the connection between the web browser and the webserver. However, this is not enough. Data stored – or as it is called in many references data at rest – is not encrypted. Therefore, users can find multiple encryption tools for stored data depending on their needs [13].

3.7 Policy Enforcement

As threats and malicious software applications on the rise, policy enforcement initiatives must be considered. Researches are made to emphasize the usage of security policies. The security policies for using mobile devices are classified to:

a) *Authentication Policy*. Where unauthorized users' accesses are prevented.
b) *Differentiating Policy*. Where all users are given different privileges based on their roles (for example administrators vs normal users).
c) *Authorization Policy*. Where some users are given access to confidential data.
d) *Integrity Policy*. Where users can access the data without tampering with it.

Without enforcing those policies and the users have not completely complied with them, mobile devices and their associated components are in danger. Once the policy is obeyed, it must be monitored and reviewed regularly. The policy should include technical, physical, and administrative concepts to cover all aspects of mobile device security [7].

4. General Guidelines to Secure Mobile Devices

As mentioned earlier, people are depending on mobile devices like smartphones in different ways. The technologies provided in this paper are more sophisticated and require professional expertise to handle them properly. However, normal users are responsible for their devices' security. Understanding the common vulnerabilities and potential attacks is critical to avoid them or at least mitigating the impact in case of attacks. Here are some of the steps that can be implemented without extreme efforts [14-17].

4.1 Using Strong Password

Almost all users are familiar with using usernames and passwords. They might be annoyed by the fact that all passwords must be difficult to guess and must be changed occasionally. However, it is important to put that into consideration when utilizing any digital device. The password should be long (eight characters at least) and complex, containing upper and lower case letters, numbers, and special characters.

4.2 Installing Antivirus Application

Mobile devices are useless without applications. Downloading applications or even different kinds of files can be risky to the device itself. Hackers intend to inject malicious codes into legitimate applications to sneak into the data inside the device or further taking control of the device later. The user must avoid such threats by installing antivirus software applications from reputable sources. These kinds of applications offer the user the needed security by removing any suspicious program or code in the device. Some versions offer wiping off the device in case of robbery or theft. Furthermore, they can delete the cookies used in browsing the Internet. These cookies can be a potential risk to the user's device because they contain sensitive information like login data and browsing information that can be accessed by other parties when being online.

4.3 Updating the Latest Software

This tip is essential. Some naïve users think that this action is luxurious, meaning that it is not necessary. However, the device's software needs to be up to date, because the old firmware usually having vulnerabilities and loopholes that might be exploited by hackers. This update comes as a security patch that the user gets automatically when connecting online. The mobile devices can schedule these updates at the user's convenience.

Other things should be considered when using mobile devices. The user needs to turn off the autofill that comes in websites and some applications. In addition, when logging on to applications linked with other applications, the user should log out from those applications immediately once finished. Finally, the applications installed in the device should be obtained from trusted stores. Many applications manifest fake interfaces that look like legitimate applications. Users need to be aware of such fraudulent applications.

5. Conclusion

Mobile devices are utilized for both personal and corporate tasks. Managing the growing functions of these devices is challenging. Due to the high processing capability of mobile devices nowadays, corporates are keeping in their minds the potential risks associated with having them inside their professional firms. This paper emphasized the critical roles that these devices play to make our lives easy and comfortable. It also discussed the associated potential risks that might sabotage the needed results from using such devices. The paper presented sophisticated technologies and recommendations to secure mobile devices. Multifactor authentication, policy enforcement, and updating the operating systems regularly are some of the best practices followed in the cybersecurity field.

It is critical to remind ourselves that there is no simple answer or measure against attacks. Attacks and threats are evolving, making it difficult for the technologies to encounter these enemies alone. It is a must for security professionals as well as business owners to take the proper proactive measures. Including developing a well-written security policy followed by training and awareness sessions for both normal staff and top management [18]. Considering the best technical, physical, and administrative controls in the cybersecurity industry.

References

[1] J. Nie, P. Wang, and L. Lei, "Why can't we be separated from our smartphones? The vital roles of smartphone activity in smartphone separation anxiety," *Computers in Human Behavior,* vol. 109, p. 106351, 2020.

[2] S. B. Utomo and B. Hendradjaya, "Multifactor authentication on mobile secure attendance system," in *2018 International Conference on ICT for Smart Society (ICISS)*, 2018, pp. 1-5.

[3] G. Kim, Y. Jeon, and J. Kim, "Secure mobile device management based on domain separation," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*, 2016, pp. 918-920.

[4] S. S. Manvi, L. B. Bhajantri, and M. Vijayakumar, "Secure mobile payment system in wireless environment," in *2009 International Conference on Future Computer and Communication*, 2009, pp. 31-35.

[5] S. Furnell, "Securing mobile devices: technology and attitude," *Network Security,* vol. 2006, pp. 9-13, 2006.

[6] A. Lima, L. Rosa, T. Cruz, and P. Simões, "A Security Monitoring Framework for Mobile Devices," *Electronics,* vol. 9, p. 1197, 2020.

[7] P. Vinayakray-Jani, "Roadmap for Securing Handheld Devices," in *IFIP International Information Security Conference*, 2003, pp. 477-482.

[8] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks," *International Journal of Engineering and Management Research,* vol. 10, 2020.

[9] H. Wang, D. Forte, M. M. Tehranipoor, and Q. Shi, "Probing attacks on integrated circuits: Challenges and research opportunities," *IEEE Design & Test,* vol. 34, pp. 63-71, 2017.

[10] E. Biagioni, "Preventing UDP flooding amplification attacks with weak authentication," in *2019 International Conference on Computing, Networking and Communications (ICNC)*, 2019, pp. 78-82.

[11] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security,* vol. 73, pp. 519-544, 2018.

[12] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Generation Computer Systems,* vol. 92, pp. 178-188, 2019.

[13] R. Hartman, C. Rokitta, and D. Peake, *Oracle Application Express for Mobile Web Applications*: Springer, 2013.

[14] B. Halpert, "Mobile device security," in *Proceedings of the 1st annual conference on Information security curriculum development*, 2004, pp. 99-101.

[15] M. A. Harris and K. P. Patten, "Mobile device security considerations for small-and medium-sized enterprise business mobility," *Information Management & Computer Security,* 2014.

[16] S. M. Dye and K. Scarfone, "A standard for developing secure mobile applications," *Computer Standards & Interfaces,* vol. 36, pp. 524-530, 2014.

[17] L. Wu, J. Wang, K.-K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Transactions on Information Forensics and Security,* vol. 14, pp. 319-330, 2018.

[18] W. L. M. A. C. M. a. P. L. P. S. h. s. i. o. The Institute of Electrical and Electronics Engineers (IEEE), ANSI/IEEE Std.802.11, 1999. (a.k.a. ISO/IEC 8802-11:1999(E)).