Mobile Device Security

Jyothy Joseph[1], Dr. K. Nirmala[2],
Research Scholar[1], Assistant Professor[2]
Quaid-E-Millath Government College for Women (Autonomous), Chennai, India[1,2]
(jyothyjoseph@gmail.com [1],nimimca@yahoo.com[2])

Abstract— Mobile Device Security refers to the protection of mobile devices and its data from various internal and external threats. This security contains both hardware and software level. It expects to protect both personal and professional information available and accessible through mobile devices. Many individuals are using mobile devices to access social networks, entertainments, media, games, e-commerce, banking and other financial activities. Many business people are using mobile devices to manage and organize their business activities in a convenient manner. This paper gives a high-level overview of Mobile device security measures and its required configurations. Presently most of the mobile device manufacturers and operating systems owners are very much keen to design and configure their mobile devices in a secured manner. The importance of mobile device security keeps trending on each period. This paper highlights various security measures, which can be implemented in Mobile devices; it includes hardware security as well as software security. The hardware security focuses the physical data security in the device, Wi-Fi networks, and Bluetooth networks, RFID (Radio Frequency Identification), NFC (Near Field Communication) and RIL (Radio Interface Layer). The software security mainly targets the operating system level security, storage level security, network security, Biometric security; Secure communication channels and secure application configurations. Here secure network mainly referred Firewall, Transport Layer Security (TLS), Virtual Private Network (VPN) and Single Sign-on (SSO). The security communication channels analysed are Secure Socket Layer (SSL), Transport Layer Security (TLS), Hyper Text Transfer Protocol Secure (HTTPS) and mVPN (mobile Virtual Private Network). The main Biometric security features analysed Fingerprints, Iris, Retina scan, auditory verification, Facial recognition, and vascular imaging. The main secure application configuration refers the secure runtime environment, Enable data security features, Proper application development and Install the applications from reliable source. This study helps the mobile device users to get a high-level interpretation of the hardware and software security measures that helps or are mandatory to use to protect their personal and professional data

Keywords-Mobile Device Security , Hardware Security, Software Security, Physical Security, Component level Security, Secure Operating system, Secure Data storage, Secure Network, Secure Applications, Secure Communication Channel, Biometric security

I. Introduction

The mobile device security targets to protect the information available in the mobile device as well as the information accessing through various applications or browsers. Many of them uphold a lot of personal information like bank account details, personal identity details, business information, photos, soft copy of documents, etc. in mobile devices. Lose of such important details from the device impact many activities in multiple ways. Now mobile apps are in trend, most of the mobiles devices contain many apps. But many of us are not ensuring its security before using the same. If the applications were not developed in a secured way or the device not capable to handle the threats, it leads to drip important information or financial loss.

II. Elaboration

Mobile device security can be enabled in two ways, hardware level as well as software level. Mobile devices required both type securities to ensure the data security as well as transaction security.

1. Hardware Security: Hardware security talks about the different security options based on hardware components of the mobile device. Nowadays few of mobile OS are validating the authenticity of hardware parts in OS level itself.

1.1 Physical Security: Physical security explains how can make safe the mobile devices from theft or loss. Below guidelines help to understand the different options and precautionary measures to secure the mobile devices

- Do not leave the mobile device in an unattended way in any of the common places.
- Always maintain the device with password protected.
- Enable backup device option if you are maintaining important information in the device.
- Enable to cloud accounts when start using the mobile device.

- If lost the mobile device, block and erase the data through the cloud account.
- Enable the find phone option in the device and trace the device through other devices or cloud account in required situations.
- If the device was stolen, immediately change the passwords of all the applications (Bank Apps, Mail account, Business Accounts, etc.) through online options.

1.2. Component level Security: Different hardware components of a mobile device have some important role to keep the device secure. Normally most of the manufacturers are using genuine hardware components to build the mobile. These components normally protect unauthorized devices and data access. Whenever any maintenance work required for the device, it would be advisable to use manufacture certified or authorized repair centres. Also if the required replacement for any of the components better to use the genuine components. Below are major hardware related security components.

- **Wi-Fi Networks:** Most of the mobile devices are enabled the Wi-Fi network feature. Users has carefully connect to the secured networks. Normally WEP, WPA, or WPA2 security features are available in Wi-Fi devices.

- **Bluetooth:** This is one of the entry points to access mobile devices. Advisable to keep disables this option whenever not required. Bluetooth is available with multiple security features like service level security and device level security.

- **RFID (Radio Frequency Identification):** RFID chips utilise radio signal for communication, normally this option will be available with enterprise devices. Increasing usage of RFID is open data threats as well as security measures. Need to use cryptographic techniques and password tags for data security.

- **NFC (Near Field Communication):** NFC allows mobile devices to communicate with near devices via radio signals. NFC works similar to RFID, but it will work only for short range. NFC features are using for many payment options. Better to keep off the NFC if not using to avoid unauthorised access attempt. In addition, keep updating the NFC related patches to avoid new threats.

- **RIL (Radio Interface Layer):** RIL allows wireless data or voice applications to communicate with a GSM/GPRS Mobile device. It provides an abstraction layer between telephony services and radio hardware.

2. **Software Security:** Software security talks about the different security options based on software components, which configured or installed in mobile devices.

2.1 Secure Operating system: Operating system offers the first layer security to mobile devices and ensuring system level confidentiality. It offers different measures to protect the operating system from various types of attacks like viruses, malware, hackers, etc. The main OS level security measures are boot-up processes, user -based permission model, process isolation, File permission, memory protection, specific runtime environments.

2.2 Secure Data storage: Secure data storage offers the data protection, which stored in device memory as well as in flash memory. Each operating system handles the data protection in a different way. Most of the operating systems are implemented the different encrypted file system methods to secure the data. Nowadays many software are available to keep the mobile device data secure. Few operating systems like iOS are giving very high priority for data security. In this operating system by default, the data are stored in an encrypted way.

2.3 Secure Network: Most of the mobile operating systems enabled different network protocols for authentication, authorisation and encrypted data communication. Majorly in two ways, the mobile devices will connect to a different network that is Wi-Fi networks and cellular networks. Below are the common network security options available in mobile devices

- **Firewall:** This is one of the commonly used option to protect the device and contains data from unauthorised accesses.
- **Transport Layer Security (TLS):** This feature is using to enable an encrypted communication channel between mobile devices and different network services.
- **Virtual Private Network (VPN):** Some of the operating systems setup a virtual private network server to enable a secure communication channel.
- **Single Sign-on (SSO):** Few of the mobile devices are enable with Single Sign-On. There are some features available to synchronize the mobile applications with device SSO- ID.

2.4 Secure Applications: Most of the mobile devices contain many applications. It might be for entertainment, multimedia, bank activities, data transfer, search etc. When installing any new application need to make sure it is

genuinely. Below are a few of common options to make sure the mobile apps genuinely.

- **Install the applications from a reliable source:** Currently, lot of applications are available in the market. Not all the applications are available in reliable sources. Hackers are normally providing different free applications in different categories to enable the hacking in installed devices. All operating systems have a secure app repository, applications are installing from those repositories is always advisable. App store for iOS, Play store for Android are examples for genuine app repository.

- **Secure runtime environment:** Applications needs to run under proper and updated run time environment. This will help to secure the devices from many external attacks. Sometimes jailbroken or rooted devices are compromising to use the original operating system runtime environment, which facilitates fraudulent activities.

- **Enable data security features:** Most of the operating systems are providing features to restrict the data access. Few operating systems are providing an option to enable the different type file or folder access when to install the application itself. In addition, keep maintaining only required access level to secured data, which will help to restrict the unauthorised access from other applications.

- **Proper application development:** The applications have to develop using right principles and apt architecture. Improper application development might cause to open the direct route to hackers to access the secured device data.

2.5 Secure Communication Channel: Privacy and security are very much essential in the mobile communication channel. When establishing any kind of communication channel at least two entities will communicate the data. If any unknown third party is monitoring the communication, it is becoming vulnerable. So mandatory need to use the right security protocols and standards.

- **Secure Socket Layer (SSL):** It is a widely used cryptographic system in mobile communication and internet browser. It provides an end-to-end encrypted communication channel. This mechanism is implementing in transport layer, it helps to provide proper handshake between the server and client.

- **Transport Layer Security (TLS):** A protocol provides privacy and data integrity between two communicating applications. It is composed of two layers, TLS Record Protocol and the TLS Handshake Protocol. The Record Protocol provides connection security, while the Handshake Protocol allows the server and client to authenticate each other and to negotiate encryption algorithms and cryptographic keys before any data is exchange.

- **Hyper Text Transfer Protocol Secure (HTTPS):** HTTPS protocol helps establish a secure communication channel to avoid eavesdropper (man in the middle) attack. This protocol is implementing in an application layer. HTTPS encrypts and decrypts user requests as well as the response that is return by the server.

- **mVPN (mobile Virtual Private Network):** Mobile VPN helps to maintain secure application sessions. It is very much effective where the users keep maintaining the applications are in open state for a long time. This is a very good mechanism to adopt changes in business communication.

2.6 Biometric security: Biometric user verification is one of the innovative security mechanism using in mobile devices based on user body parts. This mechanism uniquely identifying a person by evaluating one or more distinguishing biological traits, such as fingerprints and hand geometry. It is design to allow a user to prove the identity by providing a biometric sample and associated unique identification code in order to gain access to a secure environment. Biometric authentication cannot be duplicate as easily as username/password combinations. Below are few popular biometric verification options

- **Fingerprints:** This identification mechanism has been around for decades. This evidence does not change from birth to death and their use by law enforcement has advanced the science greatly. Recent days most of operating systems bring this security mechanism as a default feature and many of applications using this option for application authentication.

- **Iris:** Like fingerprints, Iris also unique to each individual. Iris is the coloured ring around the pupil of the eye. It is responsible for controlling the diameter and size of the pupil and the amount of light reaching the retina. Iris recognition is an automated method of biometric identification that uses mathematical pattern recognition techniques on images of the irises of an individual's eyes. Iris recognition uses a camera similar to any digital camera, to capture an image of the Iris. Iris scanning is widely accepted as a commercially viable modality.

- **Retina scan:** Retina is a part of the human eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. A retinal scan is use to map the unique patterns of a person's retina. A retinal scan is performing by casting an unperceived beam of low-energy infrared light into a person's eye. The resulting pattern of variations is convert to computer code and use for authentication. Since the retina is located at the back of the eye, retinal scanning is not widely accepted for user authentication due to the intrusive process required to capture an image.

- **Auditory verification:** Voice can be uses to identify a person. Normally voiceprint created for use of secure authentication. Voiceprint is a set of measurable characteristics of a human voice that uniquely identifies an individual. These characteristics based on the physical configuration of a speaker's mouth and throat, can be expresses as a mathematical formula. Voiceprints are uses in voice ID systems for user authentication.

- **Facial recognition:** Every face has numerous, distinguishable landmarks, the different peaks, and valleys that make up facial features. Facial recognition is able to look at a face and record its nuances such as the distance between the eyes, shape of the cheekbones and width of the nose. Taken together, these elements sketch a unique portrait of each individual.

- **Vascular imaging:** The array of our veins also provides a unique identifier. Scans of the palm or fingers are typical uses of vascular imaging for security purposes. Vascular pattern recognition uses near infrared light to reflect or transmit images of blood vessels.

Conclusion

When the usage of mobile devices is high, the importance of device security is arising proportionally. The devices users should know about the current and upcoming security threats. They can protect their device to some extent by using the default operating system level features, but that might not enough in most of the scenarios. It will be sensible to understand the basic workflow of the device and its required security feature to keep maintain the mobile device securely. When the device is using for any personal or professional functionalities, advisable to install/configure the security tools like antivirus, mVPN, SSL, etc. At the present scenario, many of them are using the mobile devices in a careless manner and most of the devices are open to the internet, so the hackers are targets the mobile devices to exploit the secure information. The awareness of the mobile device security features is essential to keep the mobile data in a secure manner. When any users plan to buy a mobile device, they can validate the available features against the expected security features to protect their data.

References

[1] T. Blitz, "Decoding mobile device security," Security, vol. 5

[2] 'Mobile OS overview' https://www.shoutmeloud.com/top-mobile-os-overview.html
[3] 'Techopedia' https://www.techopedia.com/

[4]'Wikipedia' https://en.wikipedia.org/wiki/Mobile_operating_system

[5] "More mobile security glitches," Computer Fraud & Security

[6] N.L. Clarke, S.M. Furnell & P.L. Reynolds,' Biometric Authentication for Mobile Devices

[7] M. Finneran, "Mobile security gaps abound," InformationWeek, vol. 1333, pp. 26-29, 2012.

.