ISSN No:-2456-2165

A Survey on Security Threats in Mobile Operating Systems and Existing Solutions

[1]K.G.Kaushalya Abeywardhane
Faculty of Computing
General Sir John Kotelawala Defence University
Colombo, Sri Lanka

[2]D.V.D.S.Abeysinghe
Faculty of Computing
General Sir John Kotelawala Defence University
Colombo, Sri Lanka

Abstract:- Using electronic devices has shown a significant increase in popularity in recent years all over the world. Mobile devices have taken the highest place among other electronic devices. Mobile security threats also have become a vast problem with coming new vulnerabilities of mobile devices. Here I conduct a literature review to recognize the existing threats based on different kinds of mobile operating systems and discuss the existing solutions for those threats. Another objective is to find current authentication methods used by mobile device users to protect mobile devices.

Keywords:- *Mobile, Operating System, Security, Threats.*

I. INTRODUCTION

The attractive features of the mobile devices are able to catch the child, teenagers and also elders in same manner. These features are varies from day by day according to newest technologies in the world. The mobile devices are based on different kinds of operating systems: Android,ISO, etc. and enabled to user to select the mobile devices with preferred operating system. User have the ability to select install varies kinds of applications. [15] The different kinds of social and demo graphical factors such as age [6] and gender and other technical factors like operating system features caused the usage of the different kinds of mobile devices. According to the Ericson mobility report, figure 1 shows the growth of the number of mobile subscribers and mobile subscriptions year-wise. That also proves that usage of mobile devices is increasing in billions the year to year. [7]

II. BACKGROUND OF STUDIES

Mobile Devices are considered as their personal device and use to perform day today operations. Therefore, they used to store private and sensitive data in mobile devices without thinking deeper about their security. It is easier to install different kinds of mobile applications in various kinds of operating systems such as iOS, Android, etc. Nowadays there is a big competition among mobile application providers and there are the newest more and more customized applications in today's market. Most smartphone users have practiced getting instant services through various kinds of mobile applications by inserting their very sensitive data: bank account numbers, credit card numbers and health information, etc. Those kinds of user behaviors can also increase the vulnerabilities in this field. [2] Mobile security-related threats such as mobile malicious codes are also increasing rapidly. Therefore, researchers and other mobile device companies have paid attention to protecting applications that were developed for mobile devices from the threats of vulnerabilities of mobile applications. I will work on this research to reveal the existing threats and what are the appropriate solutions and practices to overcome the different kinds of mobile threats. When comparing the mobile operating systems, the popularity of using Android-based mobile devices is higher in the world including developing countries. [2] Therefore, I conducted a literature review to find the existing mobile threats which were faced especially Android mobile users day by day and make a vulnerability analysis of Android-based mobile applications and reveal the factors that can occur in the vulnerability in mobile devices.

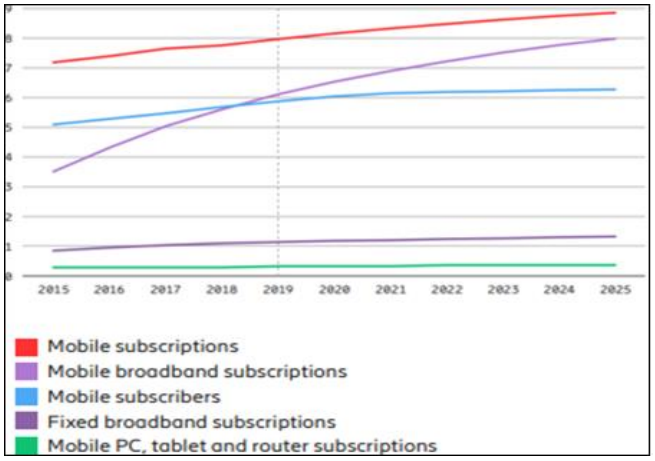

Fig 1 Subscriptions and Subscribers (Billion)

III. LITERATURE REVIEW

According to Kim, the security threats of smart devices are increasing because of increasing the usage of smart devices in the world. According to his analyzed results, vulnerabilities of applications in mobile devices are mostly caused for security threats. He used 9 mobile applications which were used by public Institutions and companies for security checks experi- ments. He has revealed that mobile applications which were used by a public institution have been used in MD5 encryption tools that may be vulnerable because of a short number of bits of MD5 and they have not properly managed the sessions of mobile applications also. Then he has proposed to produce various security check methods when developing applications for mobile devices.

He has suggested being made those kinds of security checks applications from the government side. [9] The authors in [12] have revealed security issues and threats in Android Operating System-based devices. According to their survey, there is a permission-based security mechanism in the Android system to regulate the access of third-party Android applications. That permission-based mechanism is affected to the security of the device also. They have proven that there may be information leakage in the Android systems when users grant resources without caring about any restriction from the OS.

According to the review, article which was written by Pawel Wichbroth and Lukasz Lysik, they have identified and analyzed existing threats for mobile devices and best practices for avoiding the mobile threats. They have analyzed the cur- rent mobile attacks and related security codes for preventing those mobile attacks. The world economic forum of 2019 has presented 3 technologies: 5G networks and infrastructure, artificial intelligence, and bio- metrics technology to prevent mobile threats. [15] According to Nageen Saleem and four others have proposed a solution to security threats that occur in the Android operating system. They have implemented architecture of quantum key distribution for Android-based op- erating systems to increase their efficiency of them. According to their system, the quantum key distribution method works as a guard to the Android operating system and can be used in the case of run-time kernel compromise to ensure the security of the systems. [13]

Martin Butler and Rika Butler have done research to reveal, how to affect the different kinds of mobile operating system users' behaviors to threat of mobile security. They have conducted a study to investigate the behavior of mobile users in South Africa and reveal the different kinds of operating systems like Android, iOS impact user behaviors. According to their analyzing results, the Android operating system is used widely all over the world, although there are technical issues in the Android operating system. There are common different kinds of unsafe behavior among Android users. They revealed that there was a considerable difference between users who use different kinds of operating systems and age, gender, and frequency of mobile phone use are caused to decide the behavior of mobile users. They prove that threat appraisal and a coping appraisal are influenced mobile users' threat avoidance. [2]

IV. USAGE OF MOBILE DEVICES

➢ *According to the Researchers . [7], [5], [3] the following Reasons are found to use Mobile Devices and can be Categorized as follows.*

- 73 percent of people have used mobile devices to open emails.
- Around 95 percent of users have logged into their Face- book accounts and social media accounts from mobile phones.
- 80 percent of people use mobile devices to search some information from the internet.
- Around 40 percent of people make their online transac- tions through mobile devices.

The researchers have found that the global mobile data traffic has increased by 30 exabytes per month. All these factors prove that the users of mobile devices are rapidly developing, and the following details show that mobile threats are also increasing with this growth.

V. MOBILE DEVICE SECURITY CHALLENGES

➢ *The Growth of usage of Mobile Devices is Caused to Create Various Kinds of Security Challenges also. There can be Cate- Gorized few Prominent Security Challenges because of threats and Vulnerabilities. [10]*

- Unsafe Data Storage – There may be a huge problem when losing a mobile device or affect mobile application by some malicious code because of losing sensitive data including personal information: name, address, banking information, social network addresses, work information: company name, work position, and other official docu- ments. [10]
- Mobile Browsing – most of the users use mobile devices because of the feature of mobile browsing. But normally the users are unable to see the full web address or URL. Therefore, the users are unable to determine whether the URL or web address is safe or unsafe. 32
- Multiple User Login – With the rapid growth of usage of social media, its' single sign-on (SSO) feature is created insecure status in mobile devices. Hackers can obtain, login credentials of websites or apps when users use the same login for multiple social network applications.
- Client-Side Injection - Client-Side injection: Html injec- tion, SQL injection also may be caused by to execution of some malicious programs on mobile devices. These kinds of injections can harm target files or applications on mobile devices.

VI. MOBILE THREATS AND VULNERABILITIES

Both capabilities of the hackers to hack the mobile oper- ating systems and mobile companies' security mechanisms are widening day by day. Therefore, advanced mobile security policies should be implemented to protect mobile devices from various kinds of mobile threats. Some kinds of mobile threats can be categorized as follows.

➢ *Physical Threats*

- *Bluetooth* –

The short-range radio technology (Bluetooth) which provides wireless technology for the short-range is caused to make many potential threats and vulnerabilities. When two mobile devices connect and pair the security PIN, the malicious data can be

exchanged from device to device. [1]

- *Lost Mobile Devices* –
  The malicious applications are in- cluded in the lost mobile devices and resold to the market. This will affect to spread the of malicious programs to the market. [8]

➢ *Application based Threats*

There are more downloadable applications over the internet to perform day-to-day activities through mobile devices. The malicious applications are attached to these kinds of apps and spread the malicious codes. The application-based threats can be categorized as follows.

- *Spyware* -
  These kinds of threats collect users' data without knowing their knowledge. Spyware targets to stole users' private data including contact lists, financial information, browser history, and call history data. The stolen data are used for making financial fraud. [8]

- *Malware* –
  Malware makes some malicious actions after installed to the mobile devices automatically without user approval. These types of threats are caused to make adding charges to phone bills and send unwanted messages to users. [8]

- Vulnerable Applications –
  Vulnerable applications make changes that attack to perform unwanted activities by entering users' mobile devices. [8]

- *Privacy Threats* –
  Some special features in the mobile devices global positioning system (GPS) help to attacker find the user's current location exactly. [11]

➢ *Network-based Threats*

Some kinds of network-based threats can be categorized as follows.

- *Denial of Service Attack (DoS)* –
  In these types of attacks, the attacker prevents access to applications on mobile devices. Even one attacker can make insecure the whole device by using small effort.

- *Network Exploits* –
  When the mobile device is connected to the internet, the attacker installs malicious software on the user's mobile device without the approval of the users.

- *Mobile Network Services* –
  The attacker uses mobile network services: MM, SMS, Voice Calls to gain the users' sensitive data or business data. [8]

➢ *Mobile Vulnerabilities*

Here the attacker recognizes the weak points of mobile applications and then access the flow of the device and start exploits.

- Rootkit - Rootkit malicious infects the mobile operating system by installing applications with malicious codes to the mobile devices.
- Worm - The worm is created copies of itself and spread one device to another device.
- Trojan Horse - Trojan Horse automatically install ma- licious programs to mobile devices and collects users' sensitive data through those applications.

VII. DEFENSE MECHANISM

There should be urgent attention to the current security problems and security mechanism of mobile devices to protect those devices from different kinds of threats. Therefore, there should be ensured security in all stages of the developing life cycle. Different kinds of user authentication mechanisms are shown in figure 5. Biometric authentication, token-based authentication, and knowledge-based authentication are the three fundamental approaches to all security access. Biometric IDs, physical keys, digital certificates, smart cards are used for the above security approaches. The problem is that applying those security methods is requiring high memory capacity and requesting high cost at present.

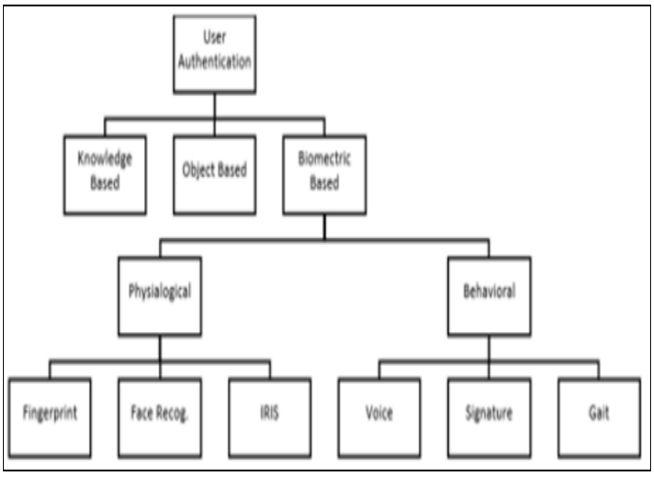

Fig 2 Different Kinds of user Authentication Mechanisms

VIII. MOBILE SECURITY BEST PRACTICES OF USERS

➢ *The Best Practices that Mobile users should be followed can be Summarized as follows.*

- Putting multi-factor authentication security methods: screen lock and unlock with PIN, fingerprint, and face recognition are considered as best practices to protect users' data.
- It is mandatory to update the mobile operating systems and mobile applications. Some kinds of applications provide regular updates to users that resolve recent vul- nerabilities and mobile threats.

ISSN No:-2456-2165

- Backing up is another approach to prevent data loss and deletion. Those kinds of activities should be done on regular basis. The user can backup the data in private or public cloud storage also
- Users can use encryption features to store data on their mobile devices. Then the authorized persons only access the data if it is needed. Survey results which were done by the authors of [14] According to the analysis report, biometric authentication methods such as fingerprint, face recognition, and iris scans provide the highest level of security.

According to the analysis which was done by the authors in [4], percent of 92 mobile users use a password or biometric protection to control the security of their smartphones. Only a percent of 37 mobile respondents disabled Bluetooth when it is not in use. Only percent of 19, downloaded and installed antivirus software on their phones. Percent of 14, respondents have downloaded and installed encryption software on their phones. According to their analysis, most smartphones are using biometric security methods to protect their data in smartphones. That means smartphone users pay attention to protecting their data or smartphones from their closest ones: family members, friends, etc. They have no proper knowledge about the vulnerabilities which come from using the internet or paring files via Bluetooth etc. Even they have not enough knowledge of what is the reason for updating the mobile operating systems. According to the survey report which was published by [15], they revealed the following percentages of security methods (shown in figure 3) that use mobile device users for their data protection. This research analysis shows that most mobile device users (percent 53.3), follow biometric security methods to protect their mobile devices. Mobile de- vices are handheld devices. Therefore, most users follow less time-consuming security methods to protect their data in those devices without thinking about their security level of them. Another point is that when using biometric security methods, the users do not memorize the PIN pattern or passwords. Those reasons are also affected to follow biometric security methods to protect the data in mobile devices. The biometric technology does not need unnecessary effort to memorize the PIN or passwords. Additionally, biometric security methods cannot be forged. But passwords and PINs can be stolen by hackers. Biometric security methods have a high ROI value thereby the organization can minimize the risk of a corporate security breach. Those reasons are also affected to follow biometric security methods to protect the data in mobile devices.

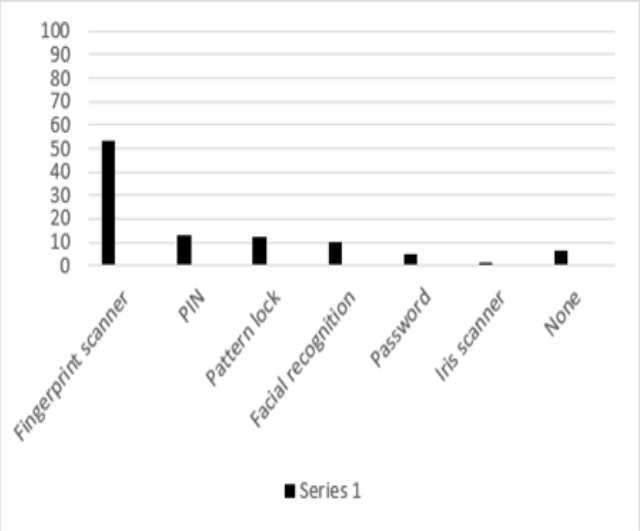

Fig 3 Percentages of Security Methods that use Mobile Device

IX. CONCLUSION

The mobile application market is growing day by day. Accordingly, the mobile security authentication mechanism also has more strength to protect mobile devices from at- tackers and hackers. Therefore, it is the responsibility of mobile device operators to apply proper security mechanisms for mobile operating systems. They should make a mobile operating system with mandatory security features which must be followed by the mobile device users. As well as it is the responsibility of every mobile user to practice authentication methods to protect their sensitive data on mobile devices. Another factor is that all mobile users do have not proper knowledge about the security of the sensitive data which they stored on their mobile devices. They used to get the service of mobile apps: mobile banking apps, online transaction apps only. Therefore, mobile developers or platform designers have more than half of the respondents to you, persons, mobile apps users follow security methods automatically. They should understand the behaviors, and perceptions of mobile device users and implemented suitable security methods to maintain the security and privacy of the data of users. Mobile device users are on different levels. They have various distances in technology or education. Therefore, by considering those kinds of factors platform designers and application developers should apply some security features to operating system levels or application levels or give the ability to install some plugins simply to users. This paper presented and analyzed the mobile security challenges at present and presented a comparison between different authentication methods. According to the literature review, the biometric authentication techniques guar- antee the highest level of security comparing various security mechanisms. The biometric authentication mechanism is easier to capture and measure the biometric features of a single person quickly. According to the conclusion of the World Economic Forum of 2019, [4-106] the three technologies: 5G network and infrastructure convergence, artificial intelligence, and biometrics for overcoming the cybercrime in future.

REFERENCES

[1]. Abhijit Bose and Kang G Shin. On mobile viruses exploiting messaging and bluetooth services. In *2006 Securecomm and Workshops*, pages 1–10. IEEE, 2006.
[2]. Martin Butler and Rika Butler. The influence of mobile operating systems on user security behavior. In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)*, pages 134–138. IEEE, 2021.
[3]. Asad Butt. 101 mobile marketing statistics and trends for 2020. January 2021.
[4]. Amita G Chin, Philip Little, and Beth H Jones. An analysis of smartphone security practices among undergraduate business students at a regional public university. *International Journal of Education and Development Using Information and Communication Technology*, 16(1):44–61, 2020.
[5]. Blue Corona. 75+ mobile marketing statistics for 2020 and beyond. December 2019.
[6]. Amit Das and Habib Ullah Khan. Security behaviors of smartphone users. *Information & Computer Security*, 2016.
[7]. SE-164 80 Stockholm Ericsson. Ericsson mobility report:subscriptions mobile data traffic co-written articles. May 2019.
[8]. Jalaluddin Khan, Haider Abbas, and Jalal Al-Muhtadi. Survey on mobile user's data privacy threats and defense mechanisms. *Procedia Computer Science*, 56:376–383, 2015.
[9]. Hee Wan Kim. A study on the mobile application security threats and vulnerability analysis cases. *International Journal of Internet, Broadcasting and Communication*, 12(4):180–187, 2020.
[10]. Andrea Pasquinucci. The security challenges of mobile devices. *Com- puter Fraud & Security*, 2009(3):16–18, 2009.
[11]. Bruce Potter. Mobile security risks: ever evolving. *Network Security*, 2007(8):19–20, 2007.
[12]. Bahman Rashidi and Carol J Fung. A survey of android security threats and defenses. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 6(3):3–35, 2015.
[13]. Nageen Saleem, Areeba Rahman, Muhammad Rizwan, Shahid Naseem, and Fahad Ahmad. Enhancing security of android operating system based phones using quantum key distribution. *EAI Endorsed Transac- tions on Scalable Information Systems*, page e10, 2020.
[14]. M Sujithra. A survey on mobile device threats, vulnerabilities and their defensive mechanism. 2012.
[15]. Paweł Weichbroth and Łukasz Łysik. Mobile security: Threats and best practices. *Mobile Information Systems*, 2020, 2020.