Available online at http://ssrn.com
SSRN-ELSEVIER (2018-2019)

International conference on "Recent Advances in Interdisciplinary Trends in Engineering & Applications

A Survey on Mobile Security Issues

Sejal Mishra[a], Archana Thakur[b]
[a,b]*School of Computer Science and IT, Devi Ahilya University, Khandwa Road, Indore – 452001, Madhya Pradesh, India*

Abstract

In today`s world of advanced science the world is changing, so is our technology. Smart- phones have become crucial part of day to day life. The increased use of smart-phones has given rise to ways we could never think like easy accessibility to net, work or personal information. But with it comes to the risk of security issues like compromised privacy or unauthorized accesses to mobile phones etc, to name some the unique structure makes easy target for malware developers and Hackers. Android for example has a very few restrictions so there is very less security system for end users. So the first target should be to eliminate these security breaches and give users the smooth experience without worrying about these problems. The paper addresses the problems faced with mobile security and how to overcome them. The paper also presents a brief description about what kind of operating system is much more at risk of these attacks and, which is more prone to security breach. It also consists of what fields still need to be researched on as to move forward in better direction. Furthermore, it explains the working of wireless systems and the attacks on it by hackers and how can that be prevented. Lastly it also illustrates about the attacks by hackers, types of attacks done on mobile phones and other related wireless systems and how to prevent them, and what users can do to prevent themselves by these attacks.

Keywords: Mobile, Security, Privacy, Wireless, Android, IOS, Smart phones.
* *E-mail address:* sejalmishra918@gmail.com

1. Introduction

Organizations depend tremendously on mobile technology; hence mobile security issues have become more vital today. Still, the security is negligible. There are more than 86 million and growing and only approximately 10% are nearly secured. [3] The security issue of devices has become hot topic for discussion but on other hand the research for the same is really few. Basically the Android is most used operating system, they are used at various places like TV, watches, cars to name a few, the main reason of popularity of android are due to its open source code licenses. There are over 2.1 Million apps in Play Store but the security for those apps to be checked is none so ever. [1][2]. The following paper represents how the need of multi-layered security is a must in this advancing world, as we need to keep our privacy intact (which may include our bank details or details of our crypto-currency or even the basic identification details) and have great accesses to the web from our phone at same time. As per the findings of this research, the need for additional layer security is a must for the single application, the need for an accurate, fast and reliable way of authentication is needed. That may include biometric systems like iris scan, fingerprint etc, in addition to passwords, pattern lock, and pin [3].

2. Related Work

Cell phones have turned into the most widely recognized methods for correspondence around the entire world. As per the most recent measurements delivered by the Central Intelligence Agency (CIA), there were 6 billion portable memberships around the world in 2011 out of a total populace of around 7 billion individuals [3].

With the quick development of technology, ruptures in framework security and occurrences of exchange misrepresentation are expanding. Therefore, there is need to build up a profound secure confirmation framework. The increasing utilization of cell phones to store a lot of information conveys the hazard of misfortune or robbery, which can trade off the security of data. This trade off of security is particularly perilous when delicate individual data is included. The present verification strategy for the security of portable gadgets relies upon the utilization of a Personal Identification Number (PIN) to confirm the client; in any case, just utilizing the rectify PIN does not ensure a person`s character. Along these lines, a more elevated amount of security is required particularly with the improvements of cell phone gadgets [4]. Current cell phones (from this time forward, called cell phones) give heaps of the abilities of customary (PCs) and, what's more, offer a substantial determination of available alternatives, for example, IEEE 802.11, Bluetooth, GSM, GPRS, UMTS, and HSPA. This plenty of engaging highlights have prompted a far-reaching dissemination of cell phones that, subsequently, is currently a perfect focus for assailants. During beginning cell phones came bundled with institutionalized Working Framework (OS): less heterogeneity in OS permitted assailants to misuse only a solitary helplessness to assault a vast number of various types of gadgets by causing significant security flare-ups [5].Some examples of the risks associated with smart phones include:

1 data leakage

2 unintentional disclosure of data attacks on decommissioned devices

3 phishing attacks

4spyware attacks

5 network spoofing attacks.

6 surveillance attacks

7 diallerware attacks

8 financial malware attacks.

9 work congestion

Portable security is the security of versatile gadgets such as, cell phones, tablets or on the other hand workstations. In this setting the center will be on brilliant telephones, which are the broadly possessed looked at to the other two. In any case of the working framework of the gadget, dangers are made against them are expanding which influence clients also, associations security. Dangers could be malware, listening in, unapproved get to, gadget theft etc. Yearly report for 2013, the organization numbers state that an increment of 42% in target assaults has been countered. This increment in digital assaults, with the increment expanded offering of convenient gadgets make the versatile security extremely vital furthermore, extremely defenseless as well [6].

Most of the apps behave like a bot on a computer i.e. like in swarm; hence mechanism used to detect bots will be irrelevant to mobile devices. Since 2009 there have been 230,000 open source forge mobile software development and like that some of the issues are unnoticed like cloned applications. There is no data as of now about how android apps repackaging can be used as assault vector, current report from F-secure reveals little insight into issue. To figure out android applications like java is straightforward, so concern for “counterfeit” android programs has been interesting issue for security [7]

.

3. Mobile Security Requirements

Let's see some basic terminologies before we go further deep into the issues. What is Hacking, Cracking, Malwares and Cybercrimes. According to an article written by Margaret Rouse, a cracker is "someone who breaches into someone else's computer system, often on a network, bypasses passwords or licenses in computer programs or in other ways intentionally breaches computer security." Cybercrime is a crime that involves the Internet, a computer system, or computer technology". ("Cybercrime") cybercriminal is someone who conducts a cybercrime. Malware is defined as any software that gets installed on your device and performs unintended tasks, often for some third party's benefit.There are some types of malware that can cause either an annoyance to the user, or steal information. These programs are known as adware and spyware. Adware is software that is supported by a program or company to show advertisements when you're online. Spyware is software that gathers information from your computer and sends it to others who would want this information. This includes such things as an bank details, product you want to buy, search history, personal data, IP address etc. [8]

Since numerous malware variations utilize IPC channels on portable stage to perform consent (benefit) heightening assaults, (for example, befuddled agent and conspiracy) I breakdown whether current methodologies deliver this zone to recognize (Furthermore, eventually) anticipate consent heightening assaults. Moreover, the investigation of the exactness of each approach i.e. its capacity to precisely recognize an assault or a powerlessness; with the negligible rate of false positive or false negatives. At long last the investigation also says whether they moreover consider the condition a gadget corporates with which is an imperative thought in Internet of Things arrangements [9].

There are two important points' for assault vectors in cellphones. First is the point at where cell phone and web connects; the second is the point where cell phone associates with a system. Since so much personal and business related information are relied on a cellphone, it makes condition of the cellphone to increase the extent of cellphones by programmers.

In the framework, there are two huge information security hazards as beneath: a.) Loss of cell phones may bargain business information and personal data which is put away in the gadgets. Individuals who blocked data would spread competitive innovations or assault servers. b.) Information block attempt amid transmission will represent risk to classification, integrity also, accessibility of information. On the off chance that the hackers altered, masked, replayed the information or influenced the server to deny the information from customer sides, the rural material vendors would manage an awesome misfortune [10].

For associations, they can build versatile security by bringing together the design of the system framework. They can bring together remote system, wired system and (VPNs) into one brought together. Profoundly secured scrambled foundation. That will help screen the system all the more intently. It will likewise enable them to recognize risk quicker than if it was decentralized. They can perform execution test utilizing moral hackers. Furthermore, Transport layer could be scrambled with a PKI (Public Key Infrastructure) to guarantee the best possible confirmation and approval is performed. In addition, introducing such programming will help battle against SMS/MMS interchanges assaults.

.*Security Requirements:*

As Mobile Cloud Computing is a combination of versatile processing and distributed computing, security hazard in portable figuring is acquired from distributed computing. Versatile distributed computing experiences the accompanying danger.

- In portable distributed computing, the client does not know where his information is put away, so the client has practically no power over the area of information.
- A client with sick expectation may plant infection of phishing assault into cloud server which may trade off information of different clients and cloud supplier will be unable to track it in view of the protection strategy of the organization.

- A hole in the security of utilization interface of cloud administrations can prompt assaults like sidestep assault of API assault.
- When cloud supplier benefits various clients, imperfection in encryption calculation can prompt unapproved access to one's information. [11]

Like conventional systems, the objectives of securing portable registering can be characterized by the accompanying characteristics: accessibility, secrecy, uprightness, genuineness and non- disavowal. By studying these parameters we also see the issues with our present working of the apps, the apps named in this list were removed by Google because they lack these characters, within last 2 months more than 100 apps were removed as they had hidden agendas for end users and breech the trust or in general terms it had virus/malwares:

- Confidentiality: ensures that the transmitted data must be gotten to by the planned beneficiaries and is never unveiled to unapproved elements. Apps removed due to this issue: Universal TV remote, USA TV 50,000, South Africa TV, ITALIA TV, SPORT TV 1.
- Availability: ensures that the planned system administrations are accessible to the proposed parties when required.
- Authenticity: allows a client to guarantee the character of the element it is speaking with. Without validation, an enemy can disguise a genuine client, along these lines increasing unapproved access to asset what's more, touchy data and meddling with the task of clients. Apps removed: Neon Pong, Tak A Trip, Join Up, Just Flashlight, Photo Editor Collage 1, Prado Parking City and Real Drone Simulator.
- Integrity: guarantees that data is never tainted amid transmission. Just the approved gatherings are ready to adjust it. Apps removed: Canais de TV do Brasil, Movies Stickers, Hearts, Prado Car, Offroad Extreme, American Muscle Car.
- Non-repudiation: ensures that a substance can demonstrate the transmission or gathering of data by another element, i.e., a sender can't dishonestly deny having gotten or sent certain information [12], [13][14].

These Apps are just a few examples of many, Google remove these types of apps on daily basis whatever maybe the reason be it a confidentiality breech or be it a malware/adware presence; these issues were reported to Google by security researchers at Trend Micro and Sophos, which we know that both of these companies are well versed in Security researches.

4. Mobile Security Issues

The basic level of problems includes:
1. Malicious applications
2. Unsafe websites
3. Data security of mobile devices
4. Network data security of the mobile devices.[15]

The other main problems are:

1. Data could incorporate usernames, Passwords, Authentication data, area administrations information,

individual data (DOB, Social security number, addresses, Visa and monetary data).

2. Frail server side control in outsider applications: This is the obligation of application designers. Every application ought to have security gauges to forestall unapproved access to the server or the application database. Moreover, to forestall spillage on client data about use of such applications.

3. Poor approval and confirmation: the utilization of legitimate validation will help distinguish unapproved code, clients or programming to be perceived and blocked.
4. Password insurance is inaccessible: Some gadgets do not have tight secret key security programming.
5. Wireless transmission isn't secured or encoded: Portable gadgets interface out in the open and private systems.

Open systems more often than not, will be not encoded thus they are not constrained to particular clients.

6. Lack of security programming for some working frameworks: Like in Bluetooth frameworks, a gadget is characterized into one of three classifications: trusted/untrusted gadget, verified/unauthenticated gadget, and obscure gadget, this is viewed as an immense hazard [16]. Under this danger there two sorts of dangers:
7. Outdated security programming: If the product isn't up and coming its database is old and not revived. The product won't distinguish new malware assaults. The helplessness of the gadget at that the increments and the security will be at the most reduced point.
8. Outdated OS: The customary updates of OS are normally bug fixes and security concerning refreshes. In the event that the framework was outdated, it will have simple purpose of access for lawbreakers and it will be effectively assaulted.
9. Unauthorized alteration "Jail breaking" or "establishing": Doing along these lines, will change the part of the application
    a. And give it an authoritative appropriate for altering and be adjusting the framework. That implies it was allowed an authorization to manage the out of this world and go. With application
    b. Validation altered and changed, assailants can without much of a stretch assault a gadget by playing with the establishing application.
10. Malware assaults: Malware a noxious programming could complete a serious mischief to cell phones. Begin from SMS instant messages spam, spam advertisements, counterfeit telephone calls, on the client cost calls and exchanges, extortion exchange to controlling the entire gadget or close it down. Malware is hazardous and could do hurt that could become about to be:
    - Denial of administration assaults: When the system ends up plainly inaccessible for the gadgets and clients in light of the noxious assault.
    - Unauthorized access: When the malware concede consent to unapproved clients to sign in a system and approach its assets.
    - Masquerade: When a malevolent programming go about as an allowed programming in a system or a gadget. As it were, put a cover to act and resemble it's the genuine application behaving. The vindictive programming takes the personality of the other specialist and act like it.
    - Eavesdropping: Eavesdropping happens when there's a convergence in a mystery or encoded correspondence between two sources.
    - Alteration: In the "NIST report of Mobile Agent security", the creators clarify adjustment as change that is made to the code of the product or the application. They expressed "When a specialist lands at an operator stage it is uncovering its code, state, and information to the stage. Since a specialist may visit a few stages under different security areas all through its lifetime,

components must be set up to guarantee the trustworthiness of the operator's code, state, and information."[17]

Mobile device threats are classified here as belonging to one out of four classes: Hardware-centric attacks, Device- independent attacks, Software-centric attacks, User layer attacks.

For these attack vectors, the different attack model is to be considered. The attack vectors investigate vulnerabilities on the victim's side, and attack models limit the power of an attacker. To distinguish between passive attackers who do not alter the content sent and active attackers who do it. Both types of attackers might have the following goals: Eavesdropping, Availability Attacks, Privacy Attacks, and Impersonation Attacks. This has been already discussed above. [18]

One of the ways that cell phones security can be enhanced is through two-advance validation framework. Two- Step Authentication consists:

A. OTP Algorithm: With a specific end goal to secure the framework, the produced OTP must be difficult to figure, recover, or followed by programmers. In this manner, it's imperative to build up a safe OTP creating the calculation. This should be present at both end that is at server and user end and create same security pattern. In recent times, all these methods are used:

- IMEI number: International Mobile Equipment Identity number is a unique number for a device and its user.
  - IMSI number: International Mobile Subscriber Identity is a unique number given to all GSM and Universal Mobile Telecommunications System (UMTS). It is to be placed in Subscriber Identity Module (SIM) card in mobile devices which can bear SIM cards.
  - Username: Although never again required on the grounds that the IMEI will exceptionally recognize the client at any rate. PIN: Personal Identification Number with any device is used to know that user is generating OTP, or with the username which is known only by the user.
- Voice based.
- Lip reading
- Image based[19]

These guarantee the right time synchronization between the two sides. For instance, in most OTP calculation the above elements are connected and the outcome is hashed utilizing SHA-256 which restores a 256 piece message. The message is then XOR-ed with the PIN recreated to 256 characters. The outcome is then Base64 encoded which yields a 28 character message. The procedure results in a secret word that is used for a moment that is only for a user. The result is more secure yet hard for user, as user has to enter each character to site or ATM. The short OTP message are user friendly but easy to be exploit by the hackers.

B. Customer Design: For a two way-advance confirmation system, information transmission, a 256-piece symmetric key are encoded for OTP calculation and sent to the server [20].

Information Security and other Security issues Cell phones are acclaimed for the vindictive code. There are numerous odds to lose or take the information since cell phones are for the most part

unprotected. An unapproved individual can undoubtedly get to the data put away on the cell phones. The best portable dangers that influence security are:

- Data misfortune from lost/stolen gadgets.
- Information-taking by portable malware.
- Data spillage through inadequately composed outsider applications.
- Vulnerabilities in gadgets, OS, plan and outsider applications.
- The insecure system gets to and temperamental access focuses.
- Insecure or maverick commercial centers.
- Insufficient administration apparatuses, capacities and access to APIs. [21]

4.1 Important Observations

The following broad observations were seen:

1. Misuse of privacy sensitive information particularly phone identifiers and geographic location. Phone identifiers, e.g., IMEI, IMSI, and ICC-ID, were used for everything from "cookie-esque" tracking to accounts numbers.
2. No evidence of telephony misuse, background recording of audio or video, abusive connections, or harvesting lists of installed applications.
3. Ad and analytic network libraries are integrated with 51% of the applications studied, with Ad Mob and Google Ads dominating.
4. No exploitable vulnerabilities that can lead malicious control of the phone were found. [22] The fundamental discoveries of investigation are abridged as takes after:
   - Third-party client following and access to delicate Android authorizations.
   - Malware nearness.
   - Traffic interference modes.
   - (Lack of) Encryption and movement spills.
   - In-way intermediaries and activity control.
   - TLC capture attempt.

The outcomes demonstrate that regardless of the guarantees of security, security and secrecy gave the dominant part of VPN applications, a large number of clients might be unconscious subject to poor security ensures and harsh practices dispensed by VPN applications. [23]

As for the overall findings with conclusion for safe practices can be noted as follows:

A. Android

- Set a device password

  PATH: Settings > Location & Security > Set up screen and Password.
- Disable Unknown Source for application installation

  PATH: Settings > Applications > Unknown sources.
- Review application permissions.
- Periodically system update.

PATH: Setting > about phone > system update > check for update.

- Turn off wireless features (GPS, Bluetooth, Wi-Fi and Portable Hotspot) when not in use

  Path: Settings > Location & Security

  Settings > Wireless & network >

  Wi-Fi Settings > Wireless &

  network > Bluetooth
- Backup data on the device

  PATH: Settings > Accounts & sync > Backup my data > time (weekly/monthly)
- Turn off Google location.
- Do not root the device.
- Web security awareness.
- Antivirus to scan Unknown sources downloads.

B. iOS

- Complex Device Password.

  PATH: Settings > General > Password/Pincode.
- Use different passwords.
- Enable Find my iphone.

  PATH: Settings > Location > Find.
- Turn on data wipe.

  PATH: Settings > General > Password limit.
- Turn off auto join wifi.
- Less Auto lock time.

  PATH: Settings > General > Autolock.
- Turn off location service
- Don’t use iCloud excessively.
- Minimize lock screen notification.

So, in order to stay protected in both of the OS these various steps can be taken, these steps reduces the chance of having any major issue by 70%. [24]

5. Conclusions

The review paper concludes that in order to prevent or defend against security issues, advanced methods should be adopted, at the following levels:

- At user level biometric system be it a fingerprint scan or iris scan, voice recognition should be used; with that user should also be taught about such malpractices in order to defend himself.
- At OS level or software developer, which can develop security protection targeted at smartphone the companies in charge should take care of its user by giving better experience of authentication like bio- metrics should become standard; in addition to pin, passwords, and pattern and knock codes. They should also increase the accuracy and anti-malware protection system in order to prevent tracing, redirecting and personal information theft.
- At the device manufacturer level, update the devices automatically so that for attackers it

would be harder to exploit security loops.

- At the network operator level, this can enhance the network infrastructure with mechanisms to avoid intrusions.
- At the level of Antivirus Database, New epidemiological models to be given to forecast if an already detected virus can initiate an epidemic.
- At the level of data transfer via wireless systems much more advanced ways should be used so that there are no breaches and data jamming and end to end encryption is maintained, iPV6 protocol should be made standard with SSL encryption and also the use of physical-layer which is quiet new innovation should be used. The use of multi-layered security should be used together to prevent the risks. Also, the data should be monitored timely for suspicious activity but without compromising the user data.

References

1. Sajid Nabi Khan, Ikhlaq Ul Firdous, 2017, Review paper on Android app security, International Journal of Advanced Research in Computer science and Software Engineering. Volume 7 Issue 4, April 2017. ISSN: 2277 128X.
2. Anjaneyulu G.S.S.N, Gayathri M. and Gopinath G, 2015, Analysis of advanced issues in mobile security in android operating system, Archives of Applied Science Research, 2015, 7(2):34-38. ISSN 0975-508X CODEN (USA) AASRC9. VIT University Vellore, India.
3. Noam Ben Asher, Hanul Sieger, Asaf Ben-Oved, Niklas Kirschnick, Joachim Meyer, and Sebastian Moller, 2011, On the Need for Different Security Methods on Mobile phones, Mobile HCL 2011, August 30 - September 2011.
4. Thamer Alhussain, Rayed AlGhamdi, Salem Alkhalaf, and Osama Alfarraj, 2013, User`s Perception of Mobile phone Security: A Survey Study In The Kingdom of Saudi Arabia, International Journal of Computer Theory and Engineering, Vol. 5, No. 5, October 2013.
5. Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, 2011, A Survey on Security for Mobile Devices, IEEE Communications Survey and Tutorials, November 2011.
6. Samaher AlJudaibi, 2015, Mobile Device Security, 2015.
7. Anjaneyulu G. S. G. N., Gayathri M. and Gopinath G., 2015, Analysis of Advanced Issues in Mobile Security in Android Operating System, Scholars Research Library, Archives of Applied Science Research, (2):34-38, ISSN 0975 – 508X, 2015.
8. Rondeau, Luke, 2014, "Mobile Device Vulnerabilities & Securities".Senior Honors Theses 381, 2014.
9. Voiletta Vylegzhanina, Douglas C. Schmidt and Jules White, 2015, Gaps and Future Directions in Mobile Security Research, MobileDeLi'2015, Vanderbilt University, Nashville, Tennessee, USA, October 2015.
10. Xiandi Zhang, Feng Yang, Zhogqiang Liu, Zhenzhi Wang and Kaiyi Wang, 2011, Research and Application of Data Security for Mobile Devices, National Engineering Research Centre for Information Technology in Agriculture Beijing China, International Federation for Information Processing 2011.
11. Sapna Malik and MM Chaturvedi, 2013, Privacy and Security in Mobile Cloud Computing: Review, International Journal of Computer Applications (0975 - 8887), Vol.80, No. 11, October 2013.
12. YuLong Zou, Jia Zou, Xianbin Wang and Lajos Hanzo, 2016, A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Journal of Proceedings of The IEEE, Priority Academic Program Devlopement , The National Natural Science Foundation, Jiangsu Province, China, Vol. 104, No. 9, September 2016.
13. T.Balasubramanian, 2015, Mobile Computing – An Introduction with Issues in Mobile Security, International Journal of Review and Research in Applied Sciences and Engineering, Vol.7, No.1, ISSN: 2231 – 0061, February 2015.
14. Sardasht Mahmood, Bakhtiar Amen and Rebwar Mala Nabi, 2016, Mobile Application Security Platforms Survey, International Journal of Computer Applications, International Journal of Computer Applications (0975 –8887) Volume 133 –No.2, January 2016.
15. P. D. Meshram Dr. R.C. Thool, 2014, A Survey Paper on Vulnerabilities in Android OS and Security of Android Devices, IEEE Global Conference on Wireless Computing and Networking (GCWCN), 2014.
16. Jun-Zhao Sun, Douglas Howie, Antti Koivisto and Jaakko Sauvola, A Hierarchical Framework Model of Mobile Security, Media Team Oulu, MVMP, Infotech Oulu, University of Oulu, Finland.
17. Mobile Application Security Platforms Survey, Sardasht Mahmood, Bakhtiar Amen and Rebwar Mala Nabi. International Journal of Computer Applications (0975 – 8887), Vol. 133, No. 2, January 2016.
18. Michael Becher, Felix C. Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck and Christopher Wolf, 2011, Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices, IEEE

Symposium on Security and Privacy 2011.

19. Fatemeh Sadat Lesani , Faranak Fotouhi Ghazvini and Rouhollah Dianat, 2015, Mobile Phone Security using Automatic Lip Reading, 9th International Conference, Qom, Iran, 16th April 2015.

20. Stefan Certic, 2014, The Future of Mobile Security, 2014.

21. M. Padma and M.Lakshmi Neelima, Mobile Cloud Computing: Issues from a Security Perspective, Monthly Journal of Computer Science and Information Technology, IJCSMC, Vol. 3, Issue 5, ISSN 2320 – 088X May 2014.

22. William Enck, Damien Octeau, Patrick McDaniel, and Swarat Chaudhuri, A Study of Android Application Security, Systems and Internet Infrastructure Security Laboratory Department of Computer Science and Engineering The Pennsylvania State University.

23. Muhammad Ikram, Narseo Vallina-Rodriguez, Suranga Seneviratne, Mohamed Ali Kaafar, Vern Paxson. 2016, An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps, IMC 2016, 14 – 16 November 2016.

24. Tae Oh, Bill Stackpole, Emily Cummins, Carlos Gonzalez, Rahul Ramachandran and Shinyoung Lim, Best Security Practices for Android, BlackBerry, and iOS, National Rehabilitation Research Institute, Seoul, South Korea.