IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Special Issue-17, May 2019 E-ISSN: 2347-2693

A Study on Wireless Mobile Phone Security Attacks and Secure Data Transfer

M. Inbavalli[1*], V. Suriya[2]

[1,2]Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur

Corresponding Author: inbavelu@yahoo.com Tel- 9442825147

Available online at: www.ijcseonline.org

***Abstract*—** Mobile phone becomes the foremost typical and fashionable mobile device in recent years. It combines the practicality of transportable and Personal Digital Assistant. Besides, it provides several computers' practicality, like process, communication, knowledge storage and etc. But, some users may be permission to allow for device and application choices. Device to attack by victimization network. The common attacks for network to security attacks, privacy attack, region attack, Phishing Network Spoofing, Desktops, etc. How to secure the mobile data to secure and protected are Device Protection, Information Protection, Application Management Security, and manage the application permission. Transferring the data use the Encryption and Decryption methods. To avoid the problems should be used for responsible websites. This is worked for only server sides and secure or install firewall in your device. Mobile firewall is used to reduce the security risk and protect the integrity of the network device.

***Keywords*—**wirelessmobile, securityattacks, secure data, encryption and decryption, firewall, applications.

I. INTRODUCTION

The phone is a key component in our life now essential. This is a Full Duplex communication and transfers the link when the user moves from one mobile device to another mobile. It's used to share the high information at a time easily but that time occur some issues. The mobile phone or smart phone now in the phone comes with a few problems or attacks. The common attacks are security attacks, privacy attack, region attack, Phishing Network Spoofing, Desktops, Bring your own device, Internet of Thing and password and Untrusted APK's. This is how we use our mobile phone safely and securely. Mobile users are must follow the instruction. There are carefully download apps and put on apps permissions. Browser stored the temporary data in cookie from user devices. Protection, Information Protection, Application-Management Security, and manage the application permissions. Transferring the data use the cryptography and secret writes strategies and, attribute based encryption.

Fig. 1. Internet communication

II. MOBILE THREATS

What is a mobile threat? Like viruses and spyware that may infect your laptop and mobile there are a range of security threats that may have an effect on mobile devices. We tend to divide these mobile threats into many categories: application and web based threats, network-based threats and physical threats.

A. Mobile Security Threat

a. Data outpouring
b. Unsecured Wi-Fi
c. Network Spoofing
d. Phishing Attacks
e. Spyware
f. Broken Cryptography
g. Improper Session Handling

Newly some additional threats to be here:
According to CXO nowadays reportage on recent Gardner information, the character of mobile security threats isn't undergoing a big modification; however the severity of the results is speedily increasing.

Pay shut attention to those 3 key impact areas:
Desktops in line with SC Magazine, a task reversal is within the works: Desktops and laptops connected to mobile

networks have become progressively chargeable for infecting mobile phones

BYOD (bring your own device). As users area unit granted high-level access from personal mobile devices , mobile phones and tablets effectively take the place of desktops—but don't supply an equivalent level of constitutional security or management.

The web of Things (IoT) With the quantity of styles of good devices—from RFID chips to thermostats and even room appliances—growing thus quickly, they can't invariably be monitored by users or antivirus solutions. As a result, hackers could use these Internet of Things devices as entry points to networks at massive.

No password protection with all of the ways that to secure mobile devices, it'd is surprising to understand that thirty-fourth of individuals do not use a word to lock their phone.

Fig. 2. Worst password

If these devices square measure lost or purloined, it provides thieves quick accesses to any or all the knowledge hold on within the phone. For those that do undergo the trouble of making a word or PIN, they usually default to codes that square measure straightforward to crack. Like 0000, 1234 or birthday month and day.

Application attacker: Attacker can be attacked by user apps. User downloaded the apps from insecure website. Attacker to attach the virus code to be applications.

Fig. 3.Security threats

B. Mobile threat statistics

Detected 1,305,015 malicious installation pack- ages, that is 439,229 l packages than within the previous quarter.

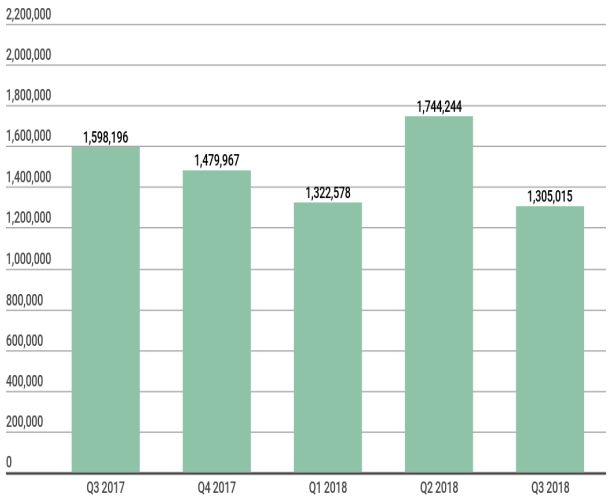

Fig. 4. *Number of detected malicious installation packages,Q3 2017-Q3 2018*

C. Distribution of detected mobile apps by kind

Among all the threats detected in Q3 2018, the lion's share belonged to likely unwanted Risk Tool apps (52.05%); compared to the previous quarter, their share shrunken by 3.3 share points (p.p.). Members of the chance Tool. Android OS. SMS reg family contributed most to the present. Second place was occupied by Trojan-Dropper threats (22.57%), whose share exaggerated by 9 p.p. Most files of this kind belonged to the Trojan-Dropper. AndroidOS. Piom, Trojan-Dropper. AndroidOS. Wapnor and Trojan-Dropper. AndroidOS. Hqwar families. The share of advertising apps continuing to decrease and accounted for 6.44% of all detected threats (compared to eight.91% in Q2 2018).

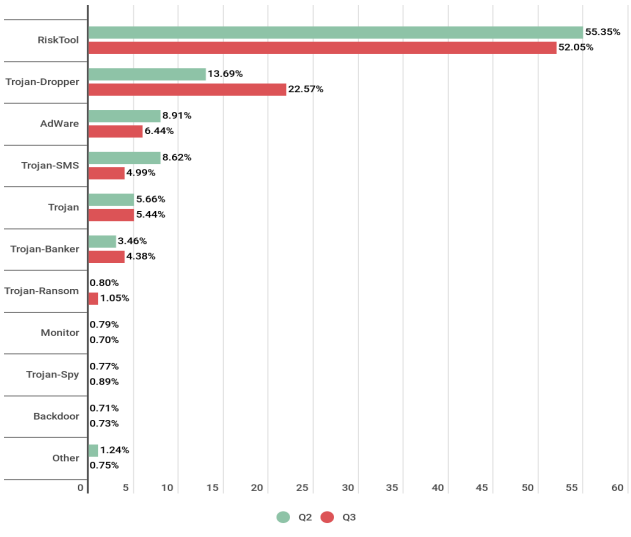

Fig. 5. *Distribution of newly detected mobile apps by type, Q2 – Q3 2018*

III. COMPARISON OF MOBILE OPERATING SYSTEM

A. Android

Android security encompasses a questionable name, in the main as a result of nobody owns it—no one regulates what will or can't be offered as associate degree automaton app, or perhaps what is sold-out as associate degree automaton phone. But, as Forbes reports, you'll be able to secure your automaton phone by keeping it updated and avoiding downloading apps of unknown or uncertain origin. Newer automaton devices support Google's automaton for Work that is meant to shield work applications and uses. Additionally, recent automaton devices from Samsung additionally support Samsung's own John Knox security technology.

Pro: Extremely configurable; you'll be able to totally management your privacy settings.
Con: Lack of standardization suggests that weak "out of the box" security.
Tip: Best if you're snug with adjusting security settings and tools.

B. Apple(IOS)

Apple's I operating system mobile software package is tightly controlled by Apple itself that additionally tightly controls the apps accessible within the Apple App Store. This management permits Apple devices to supply sensible security "out of the box," at the value of some user restrictions. For instance, iOS solely permits one copy of associate degree app on every device. Therefore, if a user encompasses a company-provided copy of associate degree app, with security restrictions in-built, the user cannot even have associate degree unrestricted version of identical app for private use.

Pro: Consistency and reliability; you recognize what you're obtaining.
Con: Not unconquerable to malware; heavily addicted to Apple security apply. Also, whereas Apple merchandise square measure usually priced above the automaton, they do not guarantee 100% security and square measure still liable to malware and hacking.
Tip: in all probability the only alternative for "pretty good" security.

C. BlackBerry

Blackberry addition- ally tightly controls devices and apps. Moreover, it's engineered for MDM, creating it easier for an organization to manage and defend its devices.

Pro: Designed to produce weapons-grade enterprise security.
Con: you may in all probability want a separate personal device, which can accompany its own security problems.
Tip: the most effective alternative if you're employed in associate degree business like finance with vital security considerations.

D. Windows Phone

Windows Phone additionally encompasses a degree of centralized management, however encompasses a history of security weaknesses, although its performance is rising as additional and additional user's square measure coming back aboard.

Pro: Compatible with Windows; steady rising security performance.
Con: History of unsure security performance within the past.
Tip: Your best bet if Windows compatibility could be a prime demand.

No one device or software package is that the definitive "best" once it involves security. However secure your smart phone is depends on your personal or skilled wants and level of school fluency. Here could be a breakdown of the professionals and cons of every variety of devices, together with a couple of things to admit once creating your decision:
Each mobile phone possibility has mobile security strengths and limitations. However, you utilize your mobile phone—and however snug you're with adjusting its security settings—will play an enormous half when making a decision that is that the best option for you, however there's little question that this dialogue can continue as additional devices come back on the market, and exaggerated security measures become additional and additional vital.

E. Other Operating System

1. Symbian OS
2. Palm OS(Garnet OS)
3. Palm webOS
4. Bada
5. Maemo OS
6. MeeGo OS

Fig. 6

IV. SECURITY PROTECTION OF MOBILE PHONE

As InfoWorld notes, all mobile phones have 3 basic components of security. Your initial major task as a mobile

user is to become awake to these layers and alter them in your devices:

A. Device Protection:
Permitting remote information "wiping" if your device is ever lost or taken. Security prompts once setting a secure lock screen. Device Protection is essentially associate sweetening of the secure lock screen. If you alter that feature and have a Google account on your phone, that account is required to access the device when a manu- facturing plant reset. Some methods to following are device protection. Use the Google play store apps and Google play protect and review the apps rate.

Firewall: The firewall could be a typical border management mechanism or perimeter defence. The purpose of a firewall is to block traffic from the surface, however it might even be accustomed to trafficking from the within. A firewall is the front line defence mechanism against intruders to enter within the system. [7]

Fig. 7.

Fig.8.

B. Information Protection:
Preventing company info from being transferred to non-public apps running on identical device or personal network. Azure info Protection(AIP), Microsoft Enterprise quality + Security (EMS) is that the entirely comprehensive resolution de- signed to help manage and defend users, devices, apps, and data in an extremely mobile-first, cloud- first world.
There are 2 general classes of key primarily based algorithms:

Symmetric encoding algorithms: it uses an equivalent key for encoding and coding. These algorithms will either operate in block mode (which works on fixed-size blocks of data) or stream mode (which works on bits or bytes of data). They're usually used for applications like encryption, file encoding and encrypting transmitted knowledge in communication networks (like TLS, emails, instant messages, etc.).

Asymmetric (or public key) encoding algorithms: not like biracial algorithms, that use an equivalent key for each encoding and coding operations, uneven algorithms use 2 separate keys for these 2 operations. These algorithms are used for computing digital signatures and key institution protocols.

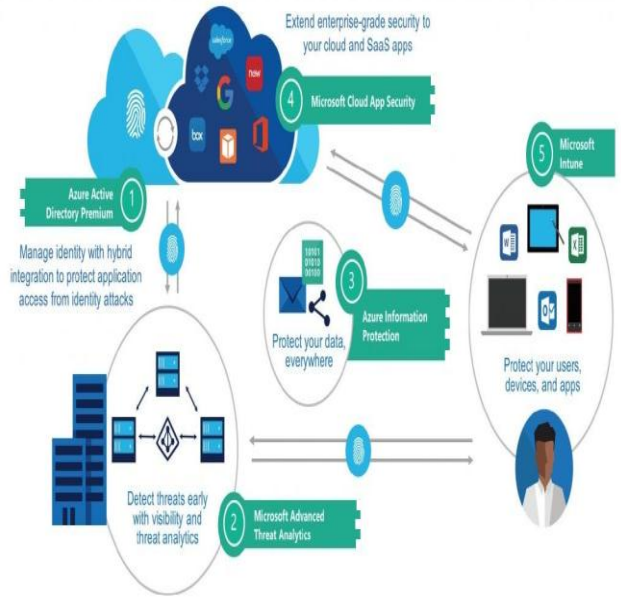

Fig.9.

1) Attribute based Encryption:
Attribute based mostly secret writing could be a kind of public-key secret writing. This ABE technique to handle the secret key of a user and the cipher text are dependent upon attributes. The decryption of a cipher text is possible only if the set of attributes of the user key matches the cipher text attributes. [4]It provides a secure way that allows data owner to share outsource data on untrusted sever

2) AES(Advanced Encryption Standard):
-Advanced Encryption Standard-To solve the DES security problems -Contest to develop a new algorithm
-Rijndel pronounced (RINE dahl) algorithm
-Won the contest and became the AES in 1999
-Key lengths have approved AES for protecting secret and top secret classified documents.
Features of AES:

a. Symmetric key symmetric block cipher
b. 128 bit data,128/192/256 bit keys
c. Provide full specification and design details

d. Software implementable in c and java

Encryption process:

a. Byte Substitution (Sub Bytes)
b. Shift rows
c. Mix Columns
d. Add round key

Decryption process:

a. Add round key
b. Mix columns
c. Shift rows
d. Byte substitution

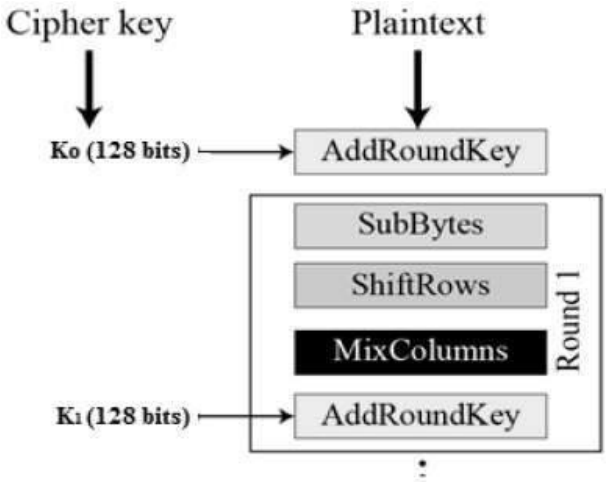

Fig. 10. Advanced Encryption Standard

The uses of encryption implement protected communications channels. It can also use for other duties/applications.

1. Cryptography Hash Function
2. Key Exchange
3. Digital Signatures
4. Certificates

C. Application-Management Security:

Protective you're in-app data from turning into compromised. Security depends not only on the phones, however additionally on the mobile device management (MDM) technology put in on company servers, which controls and manages device security. Every ought to work on to supply smart security. You would like to seem at the full image. For instance, BlackBerry Phones square measure designed and engineered for business use. Their security is great, but BlackBerry offers few widespread client apps. You would possibly want another variety of mo- bile phone for private use—including looking and banking—meaning that you just got to worry that phone's security also. The additional devices you utilize, particularly if they are connected along through the cloud or otherwise, the additional involved you ought to be for the security of your mobile network. As additional and additional apps come back onto the market, particularly for the favoured iOS and automaton phones, their security could be a growing concern regardless of that mobile device you utilize. Ira Grossman one of the specialists for Mobile technology, if doesn't have secure apps, it does not matter however secure the software package. Once professionals speak in terms of securing the complete "stack" of a tool, they're relating each the software package and also the apps it runs. Most phones have settings that enable you to verify any apps coming back from unknown sources before downloading, and as a rule of thumb, you ought to stick with the Apple, Google Play, or Microsoft stores, instead of third-party app deliverers. However, invariably browse the reviews, even within the official stores, to form positive you are not adding something suspicious to your device.

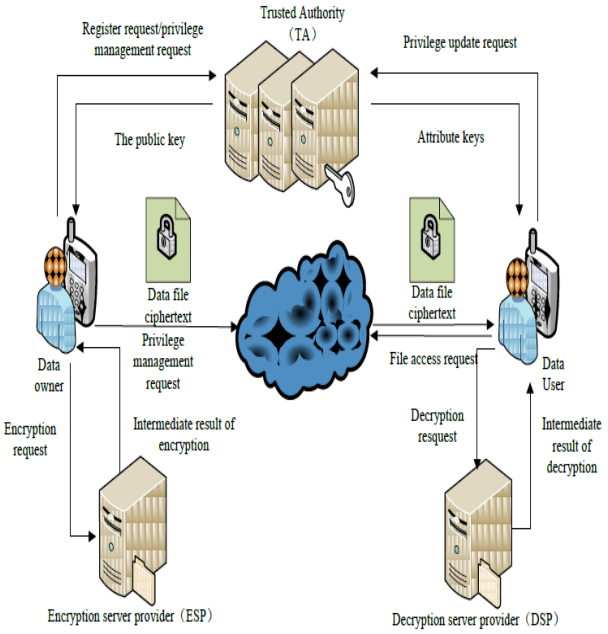

Fig. 11. Secure Data Sharing

Application Permissions: Most of the people are used the number of application without any description or analysis. They are used for unwanted apps and duplicate apps. This type of applications to theft the user data with user permission. But, user should be said to "I am not permitted my personal data access. Then how it's possible to access my mobile" Most common app permissions to below here: Contacts, Location, In-app Purchases, Phone, and Storage. In today's world wherever rarely something remains non- public, because of the insane security attacks, it's imperative that you just go back all the app permissions one by one. You'll either scrutinize them app wise or permission wise — the selection is yours. However, do confirm that it's done at once. After all,

you wouldn't need some alien stealing knowledge right from below your nose.

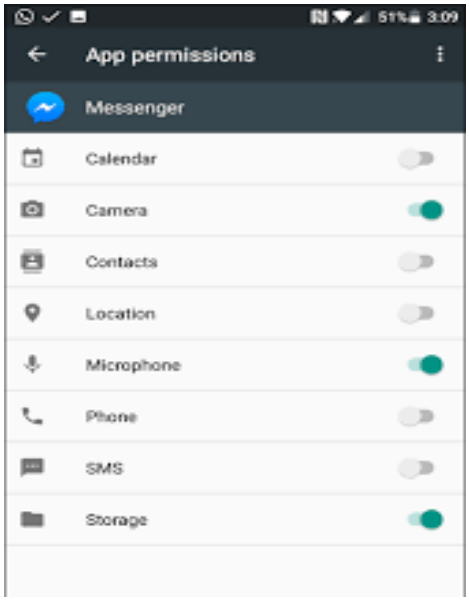

Fig. 12. Application permission

IV. CONCLUSION AND FUTURE SCOPE

If you're afraid of using apps, you can use the application. The client runs on the server side's sessions. So there is no chance of losing data or information. Some additional permission makes Apps aggressive. So some special instructions can be used. They are encryption and decryption. Do not download some antivirus to be attached in an application when downloading apps. Therefore, avoid unwanted applications and secure your data. This feature work for without applications people to use the websites or web pages. Because applications to taken high storage and previous data to stored in mobile device .it is called cookies.

REFERENCES

[1] *Manish Singh, Girish Tere "Study of Security Threats and Vulnerabilities Associated With Mobile Device"*, IJCE, Vol.1, Issue.1, Page 15, August 2016.

[2] Rajivkumar Mente and Asha Begadi *"Android Application Security", ACST, Vol.10, No.5, pp.1207-1210, ISSN 0973-6107, 2017.*

[3] Varadan,"*Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing"*, IEEE, 15 JULY 2017.

[4] *B.V.Varshini,M.VigilsonPrem,J.Geethapriya "A Review on secure data sharing in cloud computing environment",* IJARCET, Vol. 6, Issue. 3, March 2017, ISSN: 2278-1323.

[5] S.Monali Gaigole, Prof.M.A.Kalyankar *"The Study of Network Security with Its Penetrating Attacks and Possible Security Mech- anisms"*, IJCSMC, Vol.4, Issue.5, pg. 728-735, May – 2015, ISSN 2320–088X.

[6] Mohan V.Pawar, Anuradha J *"Network security and Types of Attacks in Network", Elsevier B.V, ICCC 2015.*

[7] Sardasht M.Mahmood,Bakhtiar M.Amen,Rebwar M.Nabi *"Mobile Application Security Platforms Survey"*, IJCA, Vol.133, No.2, January 2016.

[8] Md.Rakibul Hoque *"Mobile Computing Security:Issues and Requirements"*, JAIT,Vol.7, No.1, february 2016.

[9] I.Indu,P.M.Rubesh Anand,Shaicy P.Shaji *"Secure File Sharing Mechanism and key management for Mobile Cloud Computing Environment", IJST, Vol.9(48), December2016.*

[10] Syed Farhan Alam Zaidi, Munam Ali Shah, Muhammad Kamran, *"A Survey on Security for Smartphone Device"*, IJACSA, Vol.7, No.4, 2016.

[11] Vidhi B patel, Chandresh Parekh, Reena M Patel *"Encryption and Decryption Implementation method using network socket programming"*, IJARCS, Vol.8, No.5, 2017, ISSN No.0976-5697.

