Mobile Device Security

Km. Ritika[1], Ashutosh Pandey[2]
[1, 2]Dept of Computer Science & Engineering
[1, 2]ABES INSTITUTE OF TECHNOLOGY, GHAZIABAD, U.P.

Abstract*- In the era of technology mobile communication has become a necessary tool for all person[1]. A mobile device is a computing device which is small enough to hold such that it can easily operate in the hand. Now a day's mobile device used for an application like still lot of person temporize to operate mobile phones for the reason of its safety issues. Hence the mobile device security is the most important to use the mobile phone without fear of threats and vulnerability[5]. The fundamental objective of this research is to maintain the mobile phones safety and reduce mobile threats and vulnerability. This research assign with the different risk and vulnerability which can disturb the mobile device security. In this paper solution to the mobile device, security is also discussed through the biometrics authentication technique. It is noticed that 95% people have used their own mobile device Hence the security of mobile device is also the critical issue. This topic is picked out, due to growth in mobile application, mobile services .A mobile security issues are also rising Hence this research the marks the importance of mobile security and solution of mobile security issues.*

Keywords- Mobile phones security, Vulnerability, Risk, Biostatics, Mobile Device Security.

I. INTRODUCTION

Mobile phones are rapidly increase technology. It is noticed that mobile devices unit sales developed from 30 crores in 2010 to 65 crores in 2012[3]. Now a day people are doing their most of work with the help of the mobile device, such that banking, shaping business which needs sensitive data about the owner, Hence it is mandatory to provide authentic and unchallenging system for security from different vulnerability and various threats. There are the lot of security preservation which is used for purpose of security like fingerprint lock, face recognition, iris recognition all are based on biometrics authorization scheme biosensor lock play an important role in the area of mobile security with help of biometric-based user authentication we have secured our mobile device security. In 2011 250% devices activation have risen business of Google's 'play ' has exceed 11 billion and total in apps download [2].

II. MOBILE SECURITY PROBLEMS

Development of mobile phone usage and wireless technology used in mobile phone is expanded the security of mobile device has created a challenge for individual and business particularly in mobile added service like banking mobile field of government security service. There are few important challenges with the mobile device for the reason of the risk and vulnerability.

• *Bad Authorization and Authentication*

Bad authorization and authentication depend on mobile device recognition such as IMEI(International Mobile Equipment Identity), UUID(universally unique identifier). The identification of device is the reason for a hole and attacker can easily interrupted authentication and unauthorized entrance.

• *Insecure Data Storage*

Insecure data storage in mobile phone is a serious problem. Mobile Data Collection System is used to stored the data from the android mobile. Insecure data storage is mostly outcomes of non-encryption of personal detail sensitive information, for long-term storage caching of data not planned, worldwide file authorization, lead to vulnerability of secure data.

• *Security Decision via Un-trusted Inputs*

There is much application which makes security decision through user login, Hence security decision through user input can be influenced by malicious software or client-side affect for many purpose like gain information, use chargeable sensitive resources.

• *Failed Cryptography*

This problem rises through insecure expansion like as operate the custom cryptography as a replacement of the standard cryptography algorithm. Failed cryptography can conduct a broken cryptographic execution that can affect the confidentiality of sensitive and personal information.

• Client Side Injection

Client-side injection like as HTML injection and SQL injection both are related to the mobile device. clientside injection attacks may create holes with the help of these holes various functions might be accessed.

• Server Side Control

There are some server side controls like upgrades, safety configuration improving default accounts. Server side control manage the backend services that can leads to confidentiality and data integrity risks.

• Improper Session Handling

Improper session handing rises because of the user session with a extended be no longer valid time, many developers apply long or non-expiring user session that leads to improper session handling. DeLaGrange points out that "poor session management can lead to unauthorized access through session hijacking".

III. MOBILE THREATS AND VULNERABILITY

Mobile Security is essential for any mobile database. To maintain security is also most significant to secure the mobile devices, mobile phone's users and database. In mobile device wireless medium network is used for communication. wireless network is open to all person, therefore assailant can simply attack the wireless network and the mobile database. It became more insecure for the mobile user and the database of mobile phones.

3.1 MOBILE THREATS

Mobile threats are like spyware and malware that can harm your PC and mobile phones. There are many security risks that can infect mobile devices. we divide these threats as follow

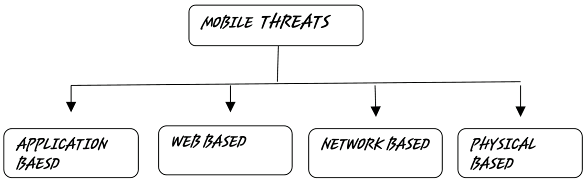

Fig1 : Various Mobile Threats

• Application-based threats
• Web-based threats
• Network-based threats
• Physical threats

Application Based Threats

There are many downloadable threats on the mobile device which can introduce many security threats. Some software specifically designed to bring harm to a mobile device. it includes following threats

• Malware
• Spyware
• Privacy threats
• Vulnerable applications

Web-Based Threats

Mobile phones are frequently link to the internet. Hence mobile devices are also used to entrance to web-based service. Web based service can cause web-based threats that produce security issues for a mobile device. There is some web-based risks.

• Party posing as a legitimate service
• Browser exploits
• Phishing scams
• Driven by downloads

Network-Based Threats

The mobile device frequently supports a cellular network and wireless network in which all attackers can easily access the network. Network Based Threats can able to unauthorized access in your networks which are follow as

• Wi-Fi sniffing
• Mobile network services
• Network exploits

Physical Threats

Mobile phones are movable and design for utilize all over the everyday lives, their physical security also the important issue which should be considered. some physical threats are follow as

• Lost or stolen mobile phones
• Computing resources
• Internet access
• Bluetooth and sharing application

Thus all above points are closely defined by the various threats.

3.2 MOBILE VULNERABILITY

In computer security, vulnerability is the combination of three constituent a system flaw, unauthorized access to the flow and assailant ability to utilize the flow. It is also defines as a weakness in a computer system itself such as the attacker, to perform unauthorized access to a computer system. A security risk influence classified as vulnerability.

An assailant must have at least one technique or tool to use vulnerability, with help of tool an attacker can connect to the system loss point. vulnerability can also called attack surface [9]. we can categorized the vulnerability follow as

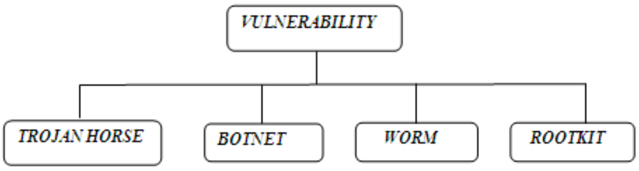

Fig 2 Various Mobile vulnerability

- Trojan horse
- Botnet
- Worm
- Rootkit

Trojan Horse

Trojan Horse is a vulnerability that can be used to gather the private information. With the help of Trojan horse phishing activities are achieved. For example, A fake application could gather personal data from the user that could harm to user.

Botnet

The Botnet is mainly used to spread Denial Of Service attack, steal data, spam send and Botnet can permit the unauthorized access the system [10]. It is the set of harm device which can be controlled remotely.

Worm

A worm is stand-alone malware program that replicates itself to increase independently to the secure system. For example the worm is IKee. B for mobile which is used to steal the sensitive data [9].

RootKit

It is a malicious software which is used to obtained right to execute a confidential mode. Rootkit detection is difficult because Rootkit accesses the administrator level.

IV. DEFENSIVE MECHANISM AND SOLUTION OF THREATS AND VULNERABILITY

All security mechanism are constructed on three basic part of data - Who you are? What you have? What do you know? [6]. Which is correlate with biometrics authentication scheme, token-based authentication technique, and knowledge-based authentication respectively. an user can give biometrics ID for identification for telling who they are? like secure ID card[7]. an user can provide a physical key or smart card for telling what they have? an user can give a password or PIN for providing what they know?[7].

There are different user authentication mechanism which is shown in fig 3

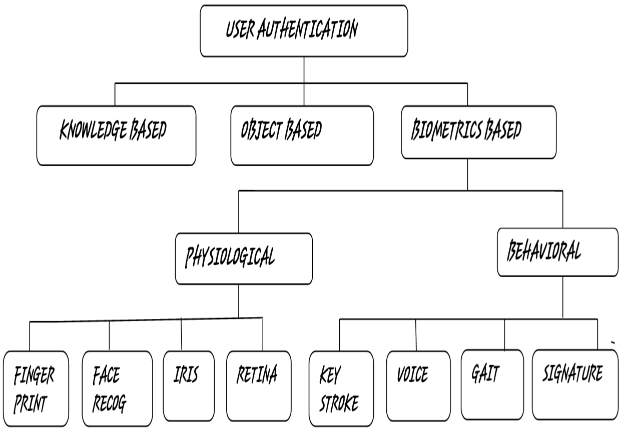

Fig3 Various Use Authentication

All above technique give the highest level of security, but these techniques have some issue with the high cost of hardware processing and memory requirements are the major issues. we have found out the user validate scheme, which are mostly focused on what you are? That is biometrics scheme. biometrics authentication scheme in the best for user authentication mobile device security. The major disadvantage of biometrics authentication that is system can be expensive and require hardware. the user is taken some measures to their mobile phones which protect a device from attacks such risks and vulnerability[8].

V. CONCLUSION

Mobile devices contain the lot of personal and sensitive information like login identity, private contact entries, invoice, purchase order among other. Hence the mobile device security is the most important issue. find new ways to get user authentication all with the increased level of security, portable computing devices are more secure after using biometrics recognition technology. Hence we can say that future of biometrics recognition technology looks brighter for mobile devices.

A Mobile devices have the camera so IRIS biometrics recognition technology is easy and guarantees high security[1].

REFERENCES

[1] Sujithra, Padmavathi, "Mobile Device Security: A Survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism" Produced for IJCA October 2012

[2] Cassandra Beyar, "Mobile Security: A Literature Review" Produced for IJCA July 2014

[3] Roberta Cozza, “Forecast: Mobile Communications Devices by Open Operating System, Worldwide, 2008-2015,” Gartner, April 5, 2011

[4] Flurry (June 2011), Mobile Application Put the Web in Their Rear-view Mirror: http://blog.flurry.com/bid/63907/Mobile- Application-Put-the- Web-in-Their-Rear-view-Mirror

[5] Google Mobile Blog, “Android and Security,” 2 February 2012. [Online]. Available: http://googlemobile.blogspot.com/2012/02/android-and-security.html. [Accessed 4 November 2012

[6] Lookout Mobile Threat Report, August 2011

[7] http://en.wikipedia.org/wiki/Vulnerability_(computing)

[8] Anurag Kumar Jain, Devendra Shanbhag “Addressing Security and Risks in Mobile Applications”.2012

[9] Paul Ruggiero and Jon Foote “Cyber Threats to Mobile ”, Produced for US-CERT, a government organization, Carnegie Mellon University-US, 2011

[10] http://en.wikipedia.org/wiki/Botnet

[11] Wiedenbeck, S.,Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Effects of tolerance and image choice, in Symposium on Usable Privacy and Security (SOUPS), at Carnegie-Mellon Univ., Pittsburgh, 6-8 July 2005.

[12] http://www.rsasecurity.com/products/securid/Last accessed in January 2008.

[13] Daniel, K. Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX UNIX Security Workshop, pp.5-14, August 1990.