ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

A Survey on Security Features Based on Some Interactions and TheirRespective Co-Operation in Handheld Devices for Communication

[1] Arogia Victor Paul M, [2] Numan Shaikh, [3] Sharon M, [4] Anil Sagar T, [5] S. Venkatesan
[1][2] M.TechI year (CNE), Dept. Of CSE, Dayananda Sagar College Of Engineering
[3] M.Tech I year(ISE), Dept. Of ISE, Dayananda Sagar College Of Engineering
[4] Asst Professor, Dept. Of CSE, Dayananda Sagar College Of Engineering
[5] Professor, Dept. Of CSE, Dayananda Sagar College Of Engineering

***Abstract*— Since from the last decade mobile communication and its usage have grown drastically, also it has become a serious business tool nowadays. Mobile devices are the major platform for the users to transfer and exchange a very huge and critical data for communication. Also most of the communications are based on handheld devices like smart phones, palmtops, tablets etc. These devices are variably used for applications like banking sector, personal digital assistance, remote login, m-commerce, e-commerce, internet access, entertainment and also medical usage. However due to usage of handheld devices rapidly, there might be a security issues which might restrict the usage of mobile devices. This article survey gives some basic glimpses about the security features such as authentication, authorization, privacy, confidentiality, and data securityin handheld devices and it briefs an idea on how to overcome various issues like threats and vulnerabilities that effect the human interactions and their cooperation using handheld devices, and also it provides various solutions to the mobile devices ensuring security.**

I. INTRODUCTION

Mobile communication are portable, they are been called as handheld communication device that are been connected to a wireless networks that allows the user to make voice calls,send messages and run applications.It is the fastest growing consumer technology,presently in 2016 there are nearing 7billion phones,tablets and PCs in use.Mobile applications are also booming over period of time,such as android users are able to choose between 2.8 million applications and Apple's give 2.2 million applications according to 2017 survey.As on increasing the number of mobile devices and the applications are growing it is giving an incentive task to attackers.In addition to financial information,mobile devices store tremendous amount of personal data and commercial data that may become the attraction for the mass-scale attacks. Thus,security is a challenge for mobile devices such as smart phones,tablets,palmtops etc. Security must be provided to mobile devices because reliability and privacy should be present.Providing security is complex.Mobile communication devices promise to greatly improve theirproductivity; and they also introduce the concept of new risks that must be maintained and managed.The further sections will be discussed about the challenges,threatsand vulnerabilities.

II. MOBILE SECURITY CHALLENGES

Mobile security has become a dominant role in mobile computing techniques and a particular concern has been taken for the security of information i.e. financial information or it may be the personal information or the commercial data stored in smart phones. Almost all users use the mobile application to perform various operations such as communication,banking,payments, and entertainment,medical usage etc.Here the huge usage of mobile is leading to welcome of new risks.Also smartmobile phones can collect and compiled for an increasing amount of sensitive information of data, for which access must be controlled to protect the data privacy of the users.All smart phones are preferred target of attacks.These attacks exploits the weakness that is present in the Smartphone's or the attackers attack by inducing malicious software's that exploits the OS or the applications due to weak knowledge of the normal users.

The below are the few mobile device security challenges because of mentioned issues.

1) Operatingsystem attacks: TheLoop holes in operating systems can create vulnerabilities that are open to attack.

2) Communication network attacks: Communications such as Bluetooth, WI-Fi,connections make device vulnerable. The communication network attack may include the following.

3) Eavesdropping: It gives the concept of an unauthorisedand real-time interception of a private communication state,such as a phone call, instant

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

messaging, and video conference or also the fax transmission.

4)Identity Spoofing:spoofing in general,is a fraudulent or malicious practise in which communication is sent from unknown sources disguised as a source known to receiver

5)Denial of Service attack: A denial of service(DoS) attack in mobile computing is an incident in which users is deprived of the services of a resource he is expected to have.With increasing mobile devices like laptops and palmtops,a new type of DoS is possible that attacks the batteriesof these devices,called "sleep deprivation attacks".

6) Sniffer attack: Packet sniffing is an act of capturing the packets of data flowing across a computer network. The software or device used to this is called as sniffer.

7)Man in the middle attack: Man in middle attack intercepts a communication between two systems.In this attack the attacker splits the connection in to two new connection one between client and attacker andthe other between attacker and server.

8) Mobile app attacks: Poor coding and improper development creates loopholes and compromise security.The most common mobile application attacks are the SQL injections and cross site scripting.

9) Malware attacks: It is nothing but malicious software.Always there is a constant rise in malware for mobile devices.The main focus of this kind of attacks is to delete important files and destroy your device. It includes Computer Viruses, Worms, Trojan Horses, Ransom Ware, Spyware and many more.

III. ATTACKS BASED ON HARDWARE VULNERABILITIES:

Hardware vulnerabilitiesare an exploitable concept that weakensin computer systems that enables to attack through certain remote or physical access to the system hardware.When a user installs software, moves files such as CD/DVD ROMS or plus in flash drives those items can all be thought of as hardware vulnerabilities. For example Row hammers (works by repeatedly rewriting memory).

Password cracking:Password managers for mobile devices are convenient.According to the survey in 2016 stolen phones cost consumers billions of dollars.

Mobile Threats and vulnerabilities: Like viruses and spyware that can infect PC,there are a various security threats that can affect mobile devices. Since wireless medium is available to allthe attacker can easily access the network and database becomes more vulnerable for users.They are divided into several categories they are

1) Application based threats.
2) Network based threats.
3) Web based threats.
4) Physical threats.

Application based threats: Applications for mobile can present many types of security issues."Malicious apps" look fine on download site,but they are specifically designed to commit fraud.Even some trusted software can be exploited for fraudulent purpose.Applications based attacks fit in one of these mentioned below.

Malware: It is nothing but malicious software,it is a Greek word,and it performs malicious actions while installed on your device. Without your knowledge these applications run in background and because a major loss to your device,the loss can also include financial one i.e. charges to your phone bill,unsolicited message to your contact list. It gives attacker control over your device.These applications can be hided in your device by the attacker.

Spyware: This software that aims to gather the information about a certain person or organisation without their knowledge;it may also the send information to another entity without the consumers consent or approval.

It is classified into four types:

1)Adware.
2)System monitor
3)Trackingcookies.
4) Trojans.

Privacy threats:These may be caused by the application that are not necessarilymalicious, butalso gather or use sensitive data information.The information can be the location,contact lists, personnel identification details.

Vulnerable applications:This means there is a defect or loop hole in an application that can be exploited for malicious purpose.Such concept of vulnerably can often allow an attacker to access sensitive data information,and perform undesirable actions,also to stop a service from functioning correctly or download the applications to your device without your knowledge.

Network based threats:network based attacks are threats that are launched and controlled from a device.Denial of service or Distributed denial of service attacks are example

Network exploits:An exploit is a piece of software, and a chunk of data, or a certain sequence of commands that takes advantage of a bug or the vulnerability in order to cause an unintended or unanticipated behaviour to occur on computer software, hardware, or something electronic types.

Wi-Fi sniffing: Cracking of a wireless networks is the defeating of security devices in the Wireless local-area networks(WLANs).it also called as Wi-Fi networks that are inherently vulnerable to the security lapses that are wired networks are exempt from in nature.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

Web based threats:A web threat is any threat that uses the World Wide Web to facilitate crime. Web threats use multiple types of malware and fraud, since mobile devices are connected to Internet and access web services it imposes a major threat for these devices.
Phishing: It is the most common threat in this a duplicate or the copy of original page will be provided to fill our credentials such as mail ids and passwords.
Drive by downloads: Automatically begins downloading an application when user visits a web page.
Browsers Exploits:A browser exploit is a form of certain malicious code that take the advantage of a flaw or the vulnerability in an operating system or software with the intent to breach browser security, and to alter browser's settings without users knowledge.
Physical Threats:Physical threats from the natural disasters,infrastructure failures,and also the malicious destruction which usually can't be predicted, and it can also cause damage to mobile devices.Mentioned below is an example of physical threat
Lost or stolen device:One of the most prevalent mobile threats.The mobile device is valuable not only because the hardware itself can be resold on the black market,but more importantlybecause of the sensitive personal and organizational information it may contain.

IV. MOBILE VULNERABILITIES

Mobile vulnerability means hackers can read texts,listen to calls and track mobile phone users.Once they have access to the signalling system7(SS7 system).A hacker can have same amount of information and snooping capability as security services.
There are top 5 Mobile application vulnerabilities.
1)**Bad data storage practise**:Inexperienced programmers have bad data storage habit.Database such as SQL make it easy to store compact data on local devices,but programmers can still store that data in clear text or in XML format,which is a readable,plain text file that makes it easy to gain access to an application's data.
2)**Malware:**Android mobile applications vulnerabilities have become a problem in part because of Google Plays open format, but also because users can side load apps,removing any oversight regarding safety of applications.Google has deployed Google Bouncer in response to malware.
3)**Unauthorised access**:After installing a mobile application users approval is required before any application can access other data or applications on an android device.Authorization is a crucial part to keep the data safe.
4)**Lack of encryption**:Application that does not use good encryption algorithms can cause problem too, because those applications can be easily breakable.Mobile application developers should use common encryption frameworks to protect user's data.
5)**Data leaks from synchronization**:In applications where users sync data to cloud,data leaks are the concern.There are many password breaches that allow the hacker to breach into many accounts.These can be overcome by making users ensure that they don't have same password for every application services.

V. TOOLS AND TECHNIQUES

There are certain tools and techniques through which that can affect mobile device security:
1)**Trojan horse**: It is a kind of mail viruses that creates backdoor to your device,when it is installed in your device.
2)**Botnet**:No of mobile devices connected to internet without the knowledge of its owner, this is helpful in case of performing DoS or DDoS attacks.
3)**Worm**:It is a self replicating virus that does not alter files in your mobile device but resides in active memory and duplicates itself.Worms use part of operating system that is automatic and usually invisible to the users.
4)**Root Kit**:It is collection of tools that enables administrator-level access to any mobile devices. A cracker install a rootkit on his device after first obtaining user level access,either by exploiting a known vulnerability or cracking a password.

VI. CONCLUSION

This article defines the system on security features based on some interactions and their respective Co-operations in handheld devices for communication with some defence construction thatare a gradually perfect and progressive development process for safety and security measures. With the mobile communication evolving to 3G/4G system, all kinds of severe potential security problems will gradually appear.Therefore, we should track the huge and very efficient development of mobile communication technology, with increase in the development of security protection and self control technology research to ensure mobile communication system operates efficiently, safely and reliably.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol4, Issue 6, June 2017

REFERENCES

[1].Mitra, S.; Acharya, T. "Gesture Recognition: A Survey," Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on, vol.37, no.3, pp.311-324, May 2007 doi: 10.1109/TSMCC.2007.893280.

[2]. J. Russell, R, Cohn, "Microsoft Voice Command", PubMix, 2012.

[3].Microsoft Kinect: http://www.microsoft.com/en-s/kinectforwindows.

[4]. A. De Luca, F. Fiacco, "Integrated control for pHRI: Collision avoidance, detection, reaction and collaboration", in: Biomedical Robotics and Biomechatronics (BioRob), 2012 4th IEEE RAS & EMBS International Conference on IEEE, 2012. p. 288-295

[5]. F. Wang, ,C. Tang, Y. Ou, Y. Xu, "A Real-Time Human Imitation System", 10th IEEE World Congress on Intelligent Control and Automation WCICA, Beijing, China, July 6-8, 2012, p. 3692-3697

[6]. S. Zolkiewski, D. Pioskowik, "Robot control and online programming by human gestures using a kinect motion sensor", In: New Perspectives in Information Systems and Technologies, Volume l. Springer International Publishing, 2014. p. 593-604.

[7]. N. H. Fang, I Li, W. Y. Wang, L. W. Lee, Y. H. Chien, "Research and design of control system for a tracked robot with a kindest sensor", in IEEE 2012 International Conference on System Science and Engineering (lCSSE), pp. 217-222, June 30-luly 2, 2012, Dalian, China.

[8]. G. Kortuem, Z. Segall, and T.G.C. Thompson, "Close Encounters: Supporting Mobile Collaboration through Interchange of User Profiles," Proc. 1st Int'l Symp. Handheld and Ubiquitous Computing (HUC99), H.-W. Gellersen, ed., LNCS 1707, SpringerVerlag, 1999, pp. 171–185

[9]. Y. Iwatani, "Love: Japanese Style," Wired News, 11 June.1998;www.wired.com/news/culture/0,1284,12899,00.html.

[10]. L. Holmquist, J. Falk, and J. Wigstroem, "Supporting Group Collaboration with Inter-Personal Awareness Devices," J. Personal Technologies, vol. 3, no. 1–2, 1999, pp. 105–124.

[11]. D. Vogel and R. Balakrishnan, "Interactive Public Ambient Displays: Transitioning from Implicit to Explicit, Public to Personal, Interaction with Multiple Users," Proc. 17th Ann. ACM Symp. User Interface Software and Technology, ACM Press, 2004, pp. 137–146.

[12]. S. Izadi et al., "Dynamo: A Public Interactive Surface Supporting the Cooperative Sharing and Exchange of Media," Proc. 16th Ann. ACM Symp. User Interface Software and Technology, ACM Press, 2003, pp. 159–168.

[13]. S.K. Card, G.G. Robertson, and J.D. Mackinlay, "The Information Visualizer, an
Information Workspace," Proc. ACM Conf. Human Factors in Computing Systems (CHI 91), ACM Press, 1991, pp. 181–188.

[14]. M. Ananny and C. Strohecker, "Designing Public Spaces for Democratic Stories," Proc. 1st ACM Workshop on Story Representation, Mechanism, and Context, ACM Press, 2004, pp. 47–50.

[15]. G.W. Fitzmaurice, "Situated Information Spaces and Spatially Aware Palmtop Computers," Comm. ACM, vol. 36, no. 7, 1993, pp. 39–49.

[16]. Anton A. Pyrkin, Member, IEEE, Alexey A. Bobtsov, Senior member, IEEE, Sergey A. Kolyubin, Graduate Student Member, IEEE, Oleg I. Borisov, Vladislav S. Gromov, Stanislav V. Aranovskiy, Member, IEEE," Output Controller for Quadcopters with Wind Disturbance Cancellation," 2014 IEEE Conference on Control Applications (CCA) Part of 2014 IEEE Multi-conference on Systems and Control October 8-10, 2014. Antibes, France

[17]. Jakob Engel, J¨urgen Sturm and Daniel Cremers," Camera-Based Navigation of a Low-Cost Quadrocopter," unpublished.