Mobile Computing and its Security

Sajid Hussain Danwar*, Saima Shoro, Raheel Hameed Sial and Muhammad Furqan
Department of Computer Science
Shah Abdul Latif University Khairpur, Sindh Pakistan
*danwersajid@gmail.com, shorosaima@gmail.com, raheelhameedsial@gmail.com, shmfurqan@gmail.com.

Abstract:

Nowadays many people are enjoying the services offered through the mobile computing, it becomes a new trend in this generation. As we all know with new devices their comes different problems same is the case with mobile computing, securing mobile computing is being difficult day by day and requires more attention from developers to secure it. From the last decade the quantity of computing machinery is increasing rapidly, integrated by increasing in their computing power has led to the increased computing devices. It allows users to communicate with different people’s from anywhere in the world and also connect us to get notification of important news, these device’s solved our so much of hard work like writing letters to the ones who are living far away from us. As we all know due to the increase of these devices there comes many problems to be dealt with the major one of them is its security and the security of data which is stored in these devices. In this paper the security issues are discussed in mobile computing and how to protect ourselves from these issues.

Keywords: Mobile Computing, Mobile Security, Mobile privacy, Data Security.

I INTRODUCTION

In this world of gadgets and devices used for communication and business purpose, the technology is used, the more likely it has also became the target of hackers. The mobile technology, particularly smart phones and tablet pc’s, which have gained so much popularity in these recent years have also the same security issues. According to different articles and authors, more than 300 million peoples were using smart phones last year, consistently the span of portable market expanded altogether, while cell phone client’s memberships assessed 7,084,987 billion by 2015 dependent on the ITU report [1]. As we all know mobile phone has become the daily life device which is being used by many people’s not just for communication purpose but also for business purpose to send and receive emails it contains our personal and confidential information which should not be disclosed or leak if it will be disclosed than it may cause serious issues to that person or his family which may also be life threatening, the Gartner which assessed “that by the end of 2010, there will be enough of factors that the risk of mobile attacks will be much greater then it’s initial days”. [2], more transformation of files are being done through smart phones to one another. Nowadays smart phones and tablet PC’s have became the daily life gadgets for accessing information, Communication and services such as emails, social networking, banking etc. Mobile applications are providing many of important

*Corresponding Author danwersajid@gmail.com
services while some of them are being released day by day to provide flexibility in daily life activities and working environment on the Go. But as we know with great features and advantages there are also some disadvantages which should be keep in mind before providing these devices to your children’s. In newspapers and articles there are many incidents being written regarding the mobile security and mobile threats which are being caused by inappropriate use of these device’s and due to basic knowledge. Because knowledge is the only source through which we can be careful enough before sharing or providing any confidential information over mobile phones and tablet pc. Before using these gadgets we must get the basic knowledge of using it appropriately in order to avoid any harm some times which can also be life threatening according to recent research many of burglary, violence, life threatening and scams are being done through these gadgets. There are many of security and privacy risks in mobile technologies, including malwares that steals our personal and confidential information from Android devices or by sending (SMS) texts to numbers, Mobile devices that have access to corporate applications, systems, and data; Addressing Security and Privacy Risks in are also due to mobile Apps that can leak our confidential information such as our mobile number, home address, photos, etc. Data security and privacy are the serious concerns for enterprises and mobile users because it will be a big loss for them if any of their data is leaked, we recently saw the first real attacks against smart phones: In March 2010, Iozzo and Weinmann evil spirit began a drive-by download assault against an iPhone 3GS that empowered an aggressor to take the SMS database from the telephone [3]. In November 2010, one of the principal open endeavors to play out an assault against the versatile program dispatched with Android was discharged [4].

In this research paper we will survey the area of Telecommunication security. This will cover all techniques that will increase the security of mobile phones and tablet pc. The contributions of this paper will help us to avoid these issues. First, we will survey the area of smart phone security. We will also use old research papers to help us understand data security and how can we secure it. Secondly, we will work on the solution to avoid data breaches through smart phone. In a summary section, this paper will include a detailed overview of different issues regarding smart phone security.

**Importance of this study**

This research paper will help students and different researcher to understand the common security issues regarding mobile computing devices and will also help them to solve or simply avoid that issues which sometimes can cause big threats to the owners of these devices and also his/her family members and sometimes these threats can be life threatening.

**II SECURITY ISSUES**

Here are some goals of security in different types of mobile computing devices which should be keep in mind before using these devices.

**Confidentiality:** In this section we must prevent unauthorized users to gain any kind of access to the critical information.

**Integrity:** In this section we ensure that no any unauthorized adjustment, obliteration or construction of information should take place.

**Availability:** In this goal we will ensure that only authorized user should get the access they want any time.

**Legitimate:** In this goal we will ensure that only authorized users should have the access to services.

**A. SECURITY RISKS OF WLANS**

Wi-Fi isn't restricted to the physical limits of a building, potential exists for unapproved access to the system from staff outside the expected inclusion zone.

The majority of safety concerns arises through this side of WLANs and divide it in to categories like as:

**B. PHYSICAL SECURITY**

As in LAN, a wire is required to connect any computer with the network, a WLAN (Wi-fi) connects different computing devices such as mobile, tablet, laptop and many other devices to the network by utilizing wireless routers. The (AP) Access Point is a device which is used to connect different devices integrated with wireless network connecters and it attaches those devices to a static network. As here is no any wires are used between the WLAN and the (AP) access point, the user’s send and receive information with the help of “air” and anyone within its range (which something like 250 feet for 802.11b/g) can simply interfere or sniff on TCP protocol to spy on message channel. Additionally, a hacker or attacker can install other devices to
generate new wireless connection by persevering it in clients or by locale up fake access point with same name. [8]

C. SECURITY REQUIREMENTS OF AD HOC NETWORKS

The objective is to shield the data and the assets from assault and misbehave. There are numerous prerequisites that a compelling security must guarantee:

Availability: The coveted system administrations must be accessible at whatever point they are normal regardless of assaults.

Authenticity: Communication between the hubs is certified. A malevolent hub can't take on the appearance of confided in one.

Data Confidentiality: Only the beneficiaries must comprehend the message however not by others that can be accomplished by cryptography.

Integrity: The message sent from hub A to hub B was not adjusted by hub C amid transmission.

Non-revocation: Ensures that a substance can demonstrate the transmission or gathering of data by another element, i.e., a sender/recipient can't erroneously deny having gotten or sent certain information. Advanced mark is utilized to guarantee nonrepudiation. [7]

D. SECURITY THREAT TO AD HOC NETWORKS

Remote worms can likewise be utilized to assault 'portable specially appointed systems', which are intended to interface gadgets, for example, cheap, low power consumed sensors utilizing short-extend remote correspondence [5]. These systems have applications in natural checking, fiasco alleviation and military tasks; when the hubs of such a framework are put in generally settled positions and there is a nearby similarity to probably the most established and best-contemplated models of infection pandemics, in view of short-term spatial contacts in two measurements.

III CONstrained NETWORK Bandwidth:

As we all know that Wi-Fi uses a lower bandwidth than the wired network (LAN). Which in result have limited size of a data to be transmitted between devices. An attacker/Hacker with proper devices and equipment can easily synflood the 2.4/5 GHz frequency, which in result will corrupt the wireless signals until the network is malfunction. Since the attackers use these attacks so that authorized users should not get the access to network services, these attacks are also known as denial of service (DoS) attack.

IV SECURITY COUNTERMEASURES

Secure Mobile computing is vital when you are going to develop any application of wireless networks, Today’s many mobile malware models contain non-technical vulnerability but by using a trick the technical security mechanisms can be override. [6]

V SIGNATURE-BASED MALWARE DETECTION

In markets the pattern-marching approach is utilized for the signature based malware detection in which the byte sequences of a program are scanned for to detect and resolve the malicious data. The malicious data is detected during compilation time. Through this approach the complete program is compiles in short time. Yet, this approach is limited because of the instruction semantics ignorance, which permits malware clouding during the program execution. [10]

VI SECURITY REQUIREMENTS

In comparison of the outdated networks, the missions of mobile computing security can be obtained through the attributes such as: Confidentiality, Integrity, Availability and Authenticity.

CONFIDENTIALITY: In this sector we must stop unofficial users to gain any kind of access to the serious information.

INTEGRITY: In this segment we make certain that no any illegal modification, destruction or designing of information should take place.

AVAILABILITY: In this objective we will make sure that only certified user should get the access they want anytime.

AUTHENTICITY: In this objective we will guarantee that only approved users should have the right to use the services. [4]

VII MOBILE COMPUTING:

In mobile computing Smart-phone provides an integrated infrastructure which integrates telecommunication onto a single resource as it
contains the mobile phones portability and features of laptop which will help us to perform any computational work on our smart phone on-the-go while we are travelling anywhere and its lighter then laptop. It also offers us Wi-Fi features to connect ourselves with the internet service and transmit our data to anyone in the world. [3]

A. DATA SECURITY IN MOBILE COMPUTING DEVICES

Data security is the major concern of any user/organization and digital products vendors because with data any digital device will be useless for professionals/businessman’s. As we all know that data plays an important role in our life specially when we are employee of any organization or individual businessman if data will be unsecure then we may face some serious circumstances such as security threats which in result sometime maybe life threatening i.e.: Loss of one’s life. And hence it is very important for us to secure our data as much as possible from any kind of data breach or theft and for that we need to be precocious without depending on any third party software’s we just need to regularly analyze any suspicious activity. To protect our data we need to follow some guidelines such as (don’t hand over your device to anyone, you must protect it by using some security patterns and pin codes, stop installing third party apps which requires many permissions etc.) [1] [11]

B. HARDWARE-ENHANCED THREAT DETECTION

Intel Threat Detection Technology (Intel® TDT) is a suite of hardware-enhanced technologies that can be incorporated into independent software vendors security solutions to augment existing capabilities and improve the detection of evolving cyber threats and exploits. Intel TDT is built into the underlying silicon and uses a combination of CPU data, machine-learning algorithms, and Intel integrated graphics for security workloads. [5]

VIII CONCLUSION

Mobile computing is a significant, developing tools. It permits mobile users to successfully link and work together with the permanent information system of an organization however remaining unconstrained by the physical location. Mobile computing is a technology being widely used in whole world more than 200million users are using mobile phones and different computing device. Hence it has become the essential part of our world and as we all know with every advantage there are also some disadvantages and security threats with it in this paper we have tried to explain each and every step to be careful from any unknown security threat. In Conclusion I would like to add that before using anyone else’s computing device and entering our personal data in it we need to be more careful because sometimes they have installed some software’s which might save your personal information data in hidden backup file for future use which in result sometime maybe very risky and he will try to blackmail/harm you by using that information in future.

REFERENCES


Engineering Technology (IJCSET), 4(04), pp.2229-3345.