INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SMART PHONES SECURITY: PROTECTION AGAINST NETWORKING ATTACKS AND DEFENSES

MR. VAIBHAV P. THAKARE[1], PROF. CHETAN J. SHELKE[2]

1. M.E. Scholar, P. R. Patil COE&T, Amravati.
2. Assistant Professor, Department Of Computer Science and Engg, P. R. Patil College of Engineering & Technology, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* In recent years Smartphone has become the most typical and popular mobile device. It acts as portable computer and functions similar to the processing unit, communication unit, data storage unit of any ordinary PC. It also provides many computers' service, such as web browser, portable media player, video call, GPS, Wi-Fi and many other applications. Due to inadequate access control policies and lack of information on securing mobile devices it is necessary to study the challenges of provisioning and managing security in mobile phone environments. However, the security of mobile communication has topped the list of concerns for mobile phone users. Confidentiality, Authentication, Integrity and Non-repudiation are required security services for mobile communication. This paper highlights various aspects of security that require extra focus when enabling mobile. This paper reviews various security issues of Smart phones.

Keywords: Smartphone, Security, Mobile communication, Authentication, OS hardening, Cellular Signaling, Phone jail-breaking, Spyware.

Corresponding Author: MR. VAIBHAV P. THAKARE

Access Online On:

www.ijpret.com

How to Cite This Article:

Vaibhav P. Thakare, IJPRET, 2016; Volume 4(9): 1375-1382

PAPER-QR CODE

INTRODUCTION

Now a days, Security is important factor in today's networking world. Security plays a very important role at the time of performing numerous operations on internet. Security is necessary in order to avoid illegal access of user's private data and information which is non-shareable and confidential. It is required in order to protect our data and available information from various types of attacks and viruses in networking for making secure transactions or any operations there is need of security. Today most of operation can takes place through internet via mobile phones or smart phones so at that time for proper operations and transactions there is need of security.

Smartphone are increasingly becoming a target of security threats. Because, the number of attacker performing browser attack is increasing recent year, whose targets are many different kinds of smart phone‟s applications. There is one kind of Trojan that can infect users' web searching engine and modify web pages or transactions. Some approaches can be used to protect users from this kind of attack, such as transaction validation, site to client authentication, security code evolution etc. [1]

1.1) What Is Attacks?

An attack is a specific technique used to exploit a valunerability. The valunerabiliis in the design of operating system and an attack could be 'Ping Of Death'. Generally there are two main types of attacks in networking.

1.1) Types Of Attacks:-

In these section we see various types of attacks which is present in the networking world.

A) Malware:-

It can be defined as malicious software which accesses mobile phones confidential information and can result in collapse of device.

Malwares can be classified as:-

a) SMS attacks: In this type, attacker can send phishing links and acquire some sensitive information such as credit/debit card number and password.

b) Bluetooth attacks: In this type of attack, users mobile location can be tracked as well as conversation can be listened by attacker by using special type of software. Attacker can also access users contact details and messages.

c) Premium rate attacks: With this type of attack, attacker can send premium rate SMSs and can make calls to premium rated number without users consent.

d) Phone jail-breaking: In this type of attack, attacker sends some attractive messages to install certain applications which can be harmful for the mobile phone.

B) SPYWARE:-

A spyware is a malicious application that pretends to be something it is not or actively hides itself from the user while collecting bits of information about the user without the users knowledge or consent. It is a spy software which hides in an application or software. It monitors victim's activities after installed and sends activity report to the attacker In this type, users personal information like call list, location, contact list can be accessed by attacker and he can physically access the device without users consent.

C) GRAYWARE:-

Though it does not cause any damage to mobile device, but it uses certain applications to access data from mobile phone for marketing purpose.

1.2) Aim:-

The basic aim of these topic to aware different kinds of attacks and viruses present in the internet world and their effects on mobile phones or smart phones, also various techniques and methods in order to prevent our important data and transactions from there harmful attacks and providing security in order to perform secure operations.

1) RELETED WORK:-

2.1) Smart Phones Network Architecture:-

Smart-phone is the trend of unified communications which integrate telecom and Internet services onto a single device because it has combined the portability of cell-phones with the computing and networking power of PCs. As illustrated in Figure 1, smart-phones, as endpoints of both networks, have connected the Internet and telecom networks together.

The architecture leans towards a GSM network but is very similar to a 3G network at least for the scope of this paper. The network consists of the Base Stations (BS), the connected Base Station Controller (BSC) (not shown in the figure), the Mobile Switching Center (MSC), the packet-data infrastructure consisting of the Serving GPRS Support Node(SGSN), the Gateway GPRS Support Node (GGSN), and the central user database the Home Location Register (HLR). The HLR keeps track of all users and their accounting information. Packet Data Protocol (PDP) setup in order to establish IP connectivity is a complex process. When a ME wishes to establish a PDP context it sends a GPRS-attach message to the SGSN. The SGSN authenticates the ME using the HLR. Next, the PDP context is established and stored at the SGSN and GGSN. This includes records and parameters for billing,quality of service information, and the IP address assigned to the specific PDP context. Maintenance and distribution of the PDP context information across the different network components is a costly process as it involves many components across the cellular network.

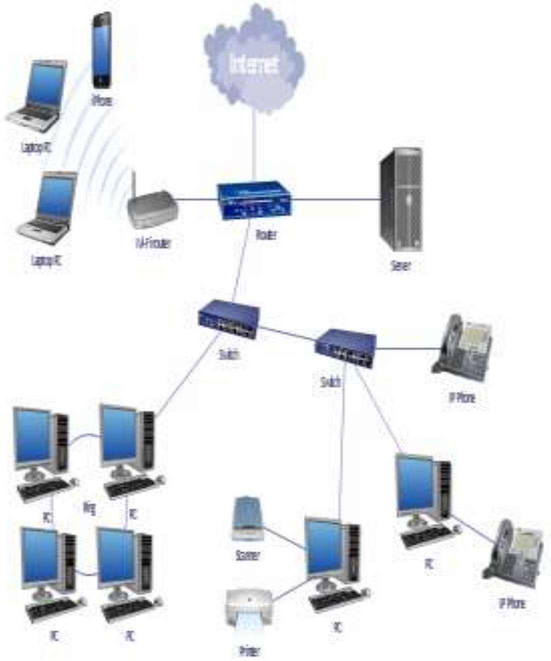

Figure 1:”Smartphone Network Architecture”.

2.2) Types Of Smart Phones Attacks:-

2.2.1) Compromising Smart-Phones:-

There are two venues for a smart-phone to be compromised:

A) Attacks from the Internet:-

Since smart-phones are also Internet endpoints, they can be compromised the same way as the PCs by worms, viruses, or Trojan horses. The first Symbian based Trojan [1] has recently been discovered in a popular game software.

B) Infection from compromised PC during data synchronization:-

Smart-phone users typically synchronize their e-mails, calendar, or other data with their desktop PCs through synchronization software like ActiveSync [5]. There exists trust relationships between smart-phones and their respective synchronization PCs. Therefore, to ultimately infect a smartphone, attackers can first infect its synchronization PC, and then the smart-phone will be infected at the next synchronization time.[7]

2.2.2) Smart-Phone Attacks against the Telecom Networks:-

A) GSM:-

GSM consists of three sub-systems: the Mobile Equipment (ME), the Base Station Subsystem (BSS), and the Network Switching Subsystem (NSS). ME has a Subscriber Identity Module (SIM) for storing identities, such as the International Mobile Subscriber Identity (IMSI). BSS consists of two elements: the Base Transceiver Station (BTS)which handles radio interfaces between BTS and MEs and the Base Station Controller (BSC) which manages radio resources and handovers. NSS uses mobile switching center(MSC) for routing phone calls and connecting the GSM system to other public networks such as PSTN.

B) SPAMMING:-

Attackers can manipulate smart-phone zombies to send junk or marketing messages through SMS. In the case that the charging model is flat, a compromised smart-phone can spam for “free”; and therefore its owner may not even notice its bad behavior. Free SMS spamming gives attackers good incentives to compromise smart-phones.[3][7]

3) DEFENSE:-

3.1) Smart-Phone Hardening:-

People have long favored functionality over security and are unwilling to pay the price and inconvenience incurred by security schemes [1]. Functionality demands extensibility, and extensibility invites malicious extensions. Given the current trend, unless legislature can effectively mandate limited extensibility for smart-phones, we don't see the hope of reducing the powerfulness and functions of a smart-phone. Nevertheless, there are some strategies that we'd like to point out for hardening smart-phone which we discuss as follows:

• Attack surface reduction:

One simple defense is to reduce the attack surface as much as possible. This defense mechanism has also been applied to PCs [4], but with limited success because it is disruptive to popular applications like file-sharing and network printer. Nevertheless, this mechanism may be more effective for smart-phones because the smart-phone usage model is different from that of PCs. Although a smart-phone is always on, most of its features need not be active. For example, when users make an outgoing phone call or compose a SMS message, the PC part of the smartphones can be turned off (unless instructed otherwise, say, when a user is downloading a movie).

• OS hardening:

Smart-phone OSes can enforce somesecurity features, such as always displaying callee's number and lighting up LCD display when dialing. This can be achieved by only exporting security enhanced APIs to applications. With hardened OSes, unless attackers can subvert the smart-phone OS without being noticed, attacking actions from malicious user-level code can be more easily detected by the smart-phone user.[3]

3.2) Internet Side Protection:-

Currently, majority of smart phones access the Internet through telecom data networks such as GPRS or CDMA1X. In this scenario, base stations can first check whether smart-phones have been properly patched or shielded and they will be forced to patch or shield if not. Alternatively, base stations could even perform shielding on behalf of the smart-phones. This kind of strategy, however, faces challenges when smart-phones use 802.11 access points for Internet connectivity: many 802.11 access points have already been deployed, it would be very difficult, if possible at all, to upgrade all the access points to enforce patching or shielding. Further, such quarantining makes seamless handoff between access networks very challenging.

CONCLUSION:-

Nowadays, mobile phones are not only restricted to voice services but also used for browsing internet, playing games, sending multimedia messages, mobile banking. Many industry professional are using their sophisticated mobile devices which helps to improve their productivity but confidential data of their enterprise moves outside of the secure perimeter of the enterprise. Therefore new security threats are emerging. As pointed out by recent research and publications, attacks on Android powered devices are becoming more sophisticated. They are now capable of spreading mechanisms which do not require explicit user confirmation. Malware may be delivered unnoticed through desktop computers, other Android devices or trojanized apps. Malicious apps cannot be avoided completely. Especially pirated apps or multimedia content in popular demand targeting user groups with typically low awareness levels are predestined to spread to many devices before being identified by Google as malware.

REFERENCES:-

1. Poornima Mahesh, Ashwini Jayawant, Geetanjali Kale On "Smartphone Security: Review of Attacks, Detection and Prevention" on 2nd International Conferenceon Electronics & Computing Technologies-2015 Conference Held at K.C.College of Engineering & Management Studies & Research, Maharashtra, India.

2. Taming Mr Hayes:" Mitigating Signaling Based Attacks on Smartphones" Collin Mulliner, Steffen Liebergeld, Matthias Lange, and Jean-Pierre Seifert Technische Universit¨at Berlin and Deutsche Telekom Laboratories D-10587, Berlin, Germany.

3. "Advanced Attacks Against PocketPC Phones"Collin Mulliner Collin trifinite.org Reliable Software Group, UC Santa Barbara & the trifinite group defcon14, August 2006.

4. "Comprehensive Security System for Mobile Network Using Elliptic Curve Cryptography over GF (p)" Lokesh Giripunje Sonali Nimbhorkarv Nagpur,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

5. P. A. Porras, H. Saidi, and V. Yegneswaran. An Analysis of the iKee.B iPhone Botnet. In Proceedings of the 2nd International ICST Conference on "Security and Privacy onMobile Information and Communications Systems (Mobisec)",May 2010.

6. Dr. S.Vijayarani1 and Ms. Maria Sylviaa. S, Assistant Professor, Department of Computer Science, Bharathiar University, Coimbatore and 2M.Phil Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore"intrusion detection system-A study"

International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015.

7. Chuanxiong Guo, Helen J. Wang and Wenwu Zhu On "Smart-Phone Attacks and Defenses".

8. Jian Cai and David J. Goodman. General Packet Radio Service in GSM.IEEE Communications Magazine, October 1997.

9. David Moore, Geoffrey Voelker, and Stefan Savage. Inferring Internet Denial-of- Service Activity. In Proceedings of the 2001 USENIX Security Symposium, 2001.

10. A. R. Beresford, A. Rice, N. Skehin, and R. Sohan. MockDroid: trading privacy for application functionality on smartphones. In 12th Workshop on Mobile Computing Systems and Applications, March 2011.