Mobile Communication: Implication Issues

Bandela Vishnuvardhan, Dr. B. Manjula
Dept. of Computer Science, Kakatiya University,
Warangal, Telangana, India-506009

ABSTRACT *- Mobile communication devices having a place with the GSM (Global System for Mobile Communications) organize ended up noticeably fit for sending and receiving instant messages. As these communication devices developed, they wound up noticeably smart, small and more features were included, for example, MMS (multimedia messaging service), which enabled users to send and get pictures. A mobile phone with highly advanced features is called a smart phone. In this paper, we carried a study on Mobile technology, services, different types of operating system, security attack (threats, malware, phishing, etc…) and various mobile network attacks.*

Keywords: - *Attacks, Mobile, Networks, Operating System, Security Challenges, Smartphone and Services.*

I. INTRODUCTION

A Mobile phone is a remote handheld device that enables users to make calls and send instant messages, among different components. The most punctual era of mobile phones could just make and get calls. The present mobile phones, be that as it may, are include with numerous extra features, for example, web programs, games, cameras, video players and even navigational frameworks systems. A mobile phone may likewise be known as a PDA or cell phone. The first cell phones were presented, their lone capacity was to make calls, and they were so massive it was difficult to convey them in a pocket.

A Mobile phone usually works on a cellular network, which is made out of cell locales scattered all through urban cities, farmlands and even hill regions. On the off chance that a client happens to be situated in a range where there is no flag from any phone site having a place with the phone arrange supplier he or she is subscribed to, calls can't be put or gotten in that area.

Mobile communication devices are progressively revolving into a basic part of human life as the best and advantageous specialized tools not limited by time and place. Mobile communication users amass rich experience of different services from Mobile applications (Google play applications, iPhone applications, and so forth) which keep running on the devices on remote servers by means of remote system frameworks.

Mobile communication technology issues include the infrastructure of protocols, mobile networks and data delivery in their use [11, 13-14]. This frame work of mobile communication is shown in below fig.1.

Current mobile devices (known as smart phones) provide variant the capabilities of ancient personal computers (PCs) and, additionally, supply an oversized choice of property choices, like IEEE 802.11, Bluetooth, GSM, GPRS, UMTS, and HSPA. This excess of appealing features has junction rectifier to a widespread diffusion of smart phones that, as a result, area unit currently a perfect target for attackers. In the starting, smart phones came packaged with standardized Operating System (OS): less heterogeneousness in OS allowed attackers to take advantage of simple vulnerability to attack an oversized number of various types of devices by inflicting major security outbreaks [1]. Recently, the amount of OSes for smart phones (Symbian OS, Windows Mobile, automaton and iPhone OS) has increased. At end of 2017 the number of mobile device users is guess to reach 4.77 billion. In end of 2019, the number of mobile phone users in the world is expected to pass the five billion mark.

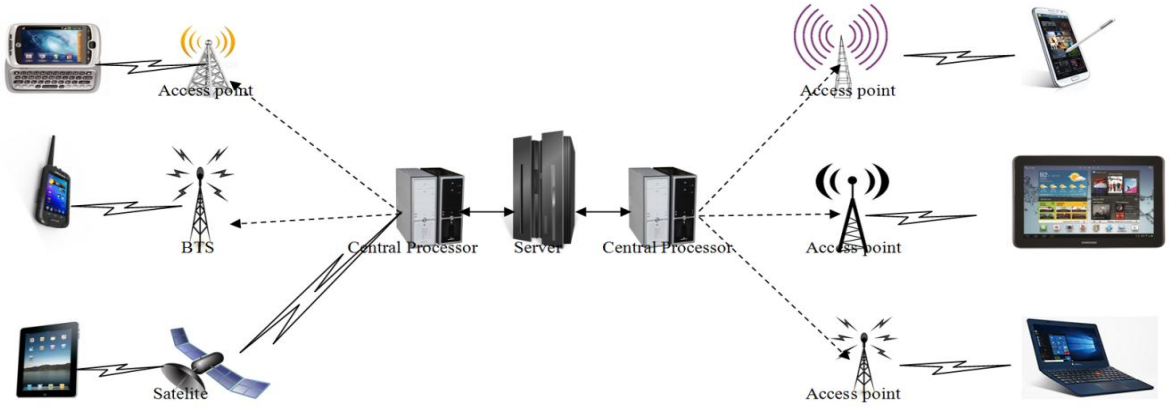

Fig.1 Mobile Communication Process

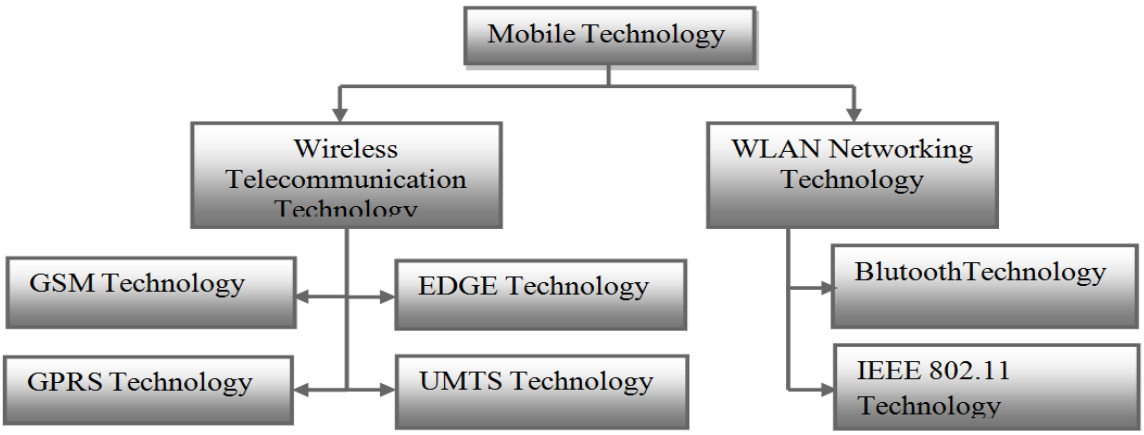

Fig.2. Various Mobile technologies

II. MOBILE TECHNOLOGY

In Global day by day technology is improved in mobile environment, have favoured the increasing smart phones as well as technologies (shown fig.2).this technologies are two types i.e Wireless telecommunication technology and WLAN networking technology.

A. Wireless Telecommunication Technology

The most necessary wireless technologies targeted at mobile communications area unit GSM, GPRS, EDGE and UMTS**.**

1) ***GSM:*** Global System for Mobile communications (GSM) is that the initial and hottest and most popular standard in Europe for mobile telecom System. GSM is a part of 2G (i.e second generation) mobile technology. It is developed in 1990 by a group Special Mobile. It is created in 1982 by Conference "CEPT (Europeenne des administrations des Postes etdes Telecommunications)", this prop up to make cellular networks wherever mobile telephones (called mobile station) communicate with each other through base stations, networks and switch subsystems**.**

2) ***GPRS:*** General Packet Radio Service (GPRS), is also known as 2.5 gen, was developed to improve network to enable users to achieve higher data rates and low access time. It is develop improve the performance of GSM. GPRS uses packet switching mechanism to exchange of data between users. This technology also supported Wireless Application Protocol (WAP) and Multimedia services.

3) ***EDGE*****:** An Enhanced Data rate for GSM Evolution was developed in 2000 to improve the features offered by GPRS by supporting higher transmission rate and higher reliability.

4) ***UMTS:*** The Universal Mobile Telecommunications System was introduced in Europe in 2002. This standard represents the third-generation (3G) on cellular system. The transmission rate is higher than 2G and 2.5G by providing a transmission speed up to 2Mbps.

B. WLAN Networking Technology

The Wireless local area networking technology (WLAN) enables devices to be networked together through wireless distribution methods and allow users to process in a local area without losing their connection to the network. There are two types of available networks in mobile environment.

1) ***Bluetooth:*** Bluetooth is a standard for the short-range wireless interconnection of mobile phones, PDAs, computers and other electronic devices. Bluetooth devices can transmit data standard range of approximately 100 meters or 328 feet.

2) ***IEEE 802.11:*** IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands [2,12].

III. MOBILE SERVICES

1) ***MTS:*** The Mobile Telephone Service (MTS) was a pre-cellular VHF radio system that links to the Public Switched Telephone Network (PSTN). MTS was the radiocellphone equivalent of land line phone service. MTS was replaced by IMTS (Improved Mobile Telephone Service). It is introduced in 1964.

2) ***IMTS:*** The Improved Mobile Telephone Service (IMTS) was a pre-cellular VHF/UHF radio system that links to the PSTN. It was introduced in 1964 as a replacement to Mobile Telephone Service or MTS and improved on most MTS systems by offering direct-dial rather than connections through a live operator [15].

IV. MOBILE OPERATING SYSTEM

Mobile Platform Operating System: The security models and development environments of the surveyed smart phone platforms are Android OS, BlackBerry OS, Symbian OS, Apple iOS, and Windows Mobile OS (Shown Fig.3). Our analysis focuses on application installation and execution. Security mechanisms that are used for the physical protection of the device are data encryption and anti-theft solutions, etc. [3].

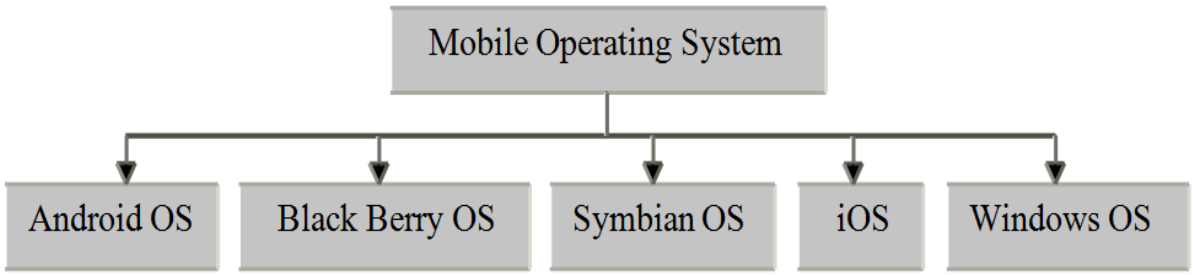

Fig.3 Mobile Operating Systems types

1) ***Android OS:*** The Android OS is a Linux based open source operating system developed and maintained by Google. Android was designed to be executed on portable devices, such as PDA, tablets and smart phones. It endow with a free of charge and openly available Software Development Kit (SDK) that includes documentation, tools and emulators necessary for the development of new applications in Java [4].

2) ***BlackBerry OS:*** The BlackBerry OS is an operating system maintained by Research in Motion Inc. (RIM). The current version of the OS is version 6. The OS is executed on BlackBerry smart phones and tablet devices created by RIM. The platform security model (RIM, 2011b) enforces restrictions to third party applications trying to access protected APIs of the OS, by demanding the signing of the application with a cryptographic key endows with by RIM (RIM, 2011a).

3) ***Symbian OS:*** Symbian OS is an operating system maintained by Nokia. Symbian is executed in smart phones and provides multiple free and publicly available SDKs. The SDK includes the tools, documentation and emulators that are necessary for the development of new applications, written in C++. The cornerstone in Symbian's security model is the use of capabilities (Nokia, 2011a) for defining restrictions to sensitive platform APIs.

4) ***iOS:*** iOS is a proprietary operating system maintained by Apple. iOS is only executed in Apple smart phones and tablets. Apple provides, after registration to the company's Dev Center (Apple, 2011a), documentation, tools and the necessary API for application development in Objective C. It should be noted that the toolset provided by Apple is only compatible with Mac OS X operating system.

5) ***Windows Mobile OS:*** Windows Mobile OS is a smart phone OS developed and maintained by Microsoft. The security model of Windows Mobile OS (Microsoft, 2010c) depends on the enabled policy of the device. This policy is responsible for controlling which applications are allowed to be executed on the device, what functionality of the OS is accessible to the application, how desktop applications interact with the smart phone, and how the user or application access specific device settings. The enabled policy on a Windows Mobile OS smart phone is either one-tier access or two-tier access [3].

V. SECURITY CHALLENGES OF MOBILE

Cellular devices including smart phones and tablets were widely used for social networking, internet browsing, calendaring, contact control, and enterprise. Mobile tool subscribers face diverse threats and attacks.

A. Threats and Attacks

Many mobile apps in smart phones/tablets cache user's secret credentials (e.g., username and password). Mobile devices are also used for banking, business, and various other purposes. They carry a great deal of sensitive data and these data should never be disclosed to an unauthorized party. The sensitive data is personal information like phone numbers, account numbers, pics, geographic location and messages. These data located in a central place in mobile device and it makes devices easy to targets for attackers. Once attack mobile device is infected by malware, it is vulnerable many threats and attacks, that attacks are shown in table 1. [5].

B. Malware Attacks

Mobile phones malware can infect devices to steal confidential data, to subscribe victims to sms premium services or turn them in to zombies. Malvertising, repackaging and update attacks are only some of the new trends mobile cyber-criminals are using to reach their victims.

1) ***Malvertising:*** It is the act of deceiving users into clicking on a rogue advertisement that leads to an exploit. This trend has spread widely with the use of social networks, although it has been present in the past in popular websites e.g. Google, FOX and Yahoo. This trend has found its way to the

mobile devices with the spread of third party applications that need sponsoring by hosting ads. GGTracker malware used Malvertising to trick Android users into visiting a fake Android market place.

2) ***Repackaging attack:*** is usually done by taking a legitimate application that has a relatively large number of users, then repackage it with the malware and republish it in another market place. DroidDream Lite malware used this technique to spread widely in 2011. Moreover, the largest botnet in China used this technique to infect more than a million devices with the Trojan Android.Troj.mdk.

TABLE 1: THREATS AND ATTACKS

Threats and Attacks		Description
Sniffing		Tapping or eavesdropping
Spam		Email spam and MMS message spam
Spoofing		Spoof the Caller ID or MMS Sender ID
Pharming		It can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.
Vishing (voice or VoIP phishing)		It is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. A vishing attack can be conducted by VoIP (voice over IP), or landline or cellular telephone or voice email.
Data leakage		Unauthorized transmission of data, intentionally or unintentionally
Vulnerabilities of Webkit engine		Vulnerability allowing attackers to crash user applications and execute code
Denial of Service	Jamming	Jamming radio channel
	Flooding	An attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
	Exhausting	Battery exhaustion attack
	Blocking	Use smart phone blocking functions to disable smart phone

3) ***Update attack:*** on the other hand, is done by creating a legitimate application, and after it has a large set of users, the malware creator will release an update with the malware in it. The Trojan DroidKungFu used this technique to infect Android devices in 2011. The danger of this attack comes from the fact that users usually won't suspect a legitimate application update to be malicious.

C. Phishing Attacks

Phishing attack is that the act of stealing personal or company data either by exploitation social engineering techniques or by exploiting a vulnerability within the device to put in a trojan or a keylogger. Within the following we'll discuss the various vectors of phishing attacks targeting smartphones and presennt a number of the solutions for every.

1) ***Mobile Browser Phishing Attacks:*** Mobile browser phishing attacks are all phishing attacks that target browsers along with phishing attacks that are specifically crafted to attack mobile browsers. Mobile browsers ack many security features found in the regular browsers because of the inherent limitations of the mobile devices.

2) ***Application Phishing Attacks:*** Mobile application phishing attacks are the phishing attacks targeted by smart phone applications other than the browser. In this case, the user will be enticed to download a rogue application that imitates a legitimate one. The malicious app will then collects the user's credentials and sensitive data. This is especially dangerous when it comes to mobile banking applications. These applications make it easy to perform financial transactions on the go. That is why they are becoming more popular than accessing the bank's website from the browser.

3) ***SMiShing Attacks:*** SMS messages have became the number one communication method in most parts of the world, and their use has exceeded the use of emails. Consequently, the number of SMS

spam is increasing 500% on a yearly basis, which led to the drastic growth of phishing SMS (SMiShing), as records show in September 2012. These SMiShing attacks usually trick victims to respond by either visiting a fraudulent website, or calling a fraudulent number. Once the victim visits the website or answers the phone call, he/she will be enticed into providing personal or financial information such as bank [6].

D. Other Attacks

1) ***Break-in attacks:*** The attacks are enabling the attacker to gain control over the targeted device by exploiting either programming errors.

2) ***Infrastructure-based attacks:*** The services provided by the infrastructure are the basis for essential smart phone functionalities, such as placing/receiving calls, SMS, email service. The attacks are like GPRS attacks, UMTS attacks etc.

3) ***Worm-based attacks:*** A worm is a program that makes copies of itself, typically from one device to another one, using different transport mechanism through an existing network without any user intervention.

4) ***Botnets:*** Botnet is a set of devices that are infected by a virus that gives an attacker the ability to remotely control them [2].

VI. MOBILE NETWORK ATTACKS

Many different kind of wireless attacks against smart phones, especially those target personal and sensitive data. In cellular networks having different kind of attacks, vulnerabilities and threats in 2G to 5G.

A. Attacks in 2G-Networks

Security vulnerabilities in 2G networks include: the obscurity, meaning that none of the security algorithms used by GSM is available to the public, provision of access security only, weak and difficult to upgrade cryptographic mechanisms, mobile subscriber visibility missing, and authentication of user to the network and not vice versa [7]. In addition, there are two classes of security requirements for 2G networks: for mobile user's privacy and data integrity protection.

The most common types of attacks and vulnerability exploits in these types of networks are:

1) ***GSM security flaws -*** no authentication of the network is provided to the end user; vulnerabilities in the subscriber identity confidentiality mechanism.

2) ***Impersonation attacks*** - the attacker tends to impersonate a legitimate user for conducting an attack.

3) ***The attack gains anonymity*** - the attacker gains information on the user's habits, calling patterns, etc., which can be used against the end user.

4) ***The attacks against confidentiality*** - the attacker uses weaknesses in the GSM architecture, flaws in the protocols between the GSM networks and the end user; major attacks of the type are brute force attacks, cryptanalysis based attacks, and non-cryptanalysis attacks.

5) ***Denial of Service (DoS) attacks*** - is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet**.**

B. Attacks in 3G-Networks

The 3G network communication provides global roaming, high bandwidth and protection on services to the users.

1) ***Interception attacks:*** The attacker catches data or peruses indicatating messages, yet does not alter or erase them. Such attacks affect the security of the subscriber and the system network operator.

2) ***Fabrication/Replay attacks:*** The attacker may insert spurious objects into the system that depend on the target means and physical access type (e.g., fake service logic, fake subscriber data or signalling messages).

3) ***Resources modification*:** The attacker origin damage by modifying system resources.

4) ***Service Logic attacks:*** The attacker causes important damages by simply attacking the service logic running in the various 3G network entities.

5) ***Eavesdropping:*** The attacker intercepts messages without detection.

C. Attacks in 4G-Networks

4G wireless technologies are intended to operate entirely on the IP architecture and suite of protocols; it increases consequences regarding the security issues. Long Term Evolution (LTE) is one of the technologies that are considered to achieve the 4G wireless.

1) ***Interference:*** The attacker deliberately inserts man made interference on to a medium that cause communication system to stop functioning due to the high signal to noise ratio.

2) ***Scrambling:*** The form of interference which is activated for short time intervals. It is targeted at the specific frame odd parts of frames, i.e., management or control information in order to disrupt a service. This attack is very difficult to launch successfully

3) ***Location tracking:*** The attacker tracks the presence of user equipment in a particular cell or across multiple cells, and although it does not represent a direct security threat, it definitely is a security breach in the network which can be viewed as potential threat.

4) ***Bandwidth stealing:*** The attacker achieves the attack by inserting messages during the Discontinuous Reception (DRX) period or by utilizing fake buffer status reports [8].

D. Attacks in 5G-Networks

In 5G cellular network architecture as some of the key emerging technologies, that are helps in improving the architecture and meeting the demands of users. Access Beam division multiple access (BDMA) and non- and quasi-orthogonal or filter bank multi carrier (FBMS) access [9]. It is important to understand that today in 2016; 5G is not a technical standard. Instead it is defined by a set of aspirations around desired services intended to be commercially available around 2020. These services are expected to place new requirements on flexibility, cost efficiency and connectivity performance. Some companies have already announced that they intend to launch 5G capable networks commercially in 2018.

Femtocell attacks:

1) Physical tampering with equipment (interference with other devices).
2) Configuration attacks (mis configuration of ACL)
3) Protocol attacks (MitMduring first access)
4) Attacks on mobile operator's core network from compromised nodes
5) Credential theft, user data and identity privacy attacks from open access nodes
6) Attacks on radio resources and management to increase handover

VII. CONCLUSION

Mobile phone and tablets are widely used for personal and business uses. A mobile device may carry a great deal of sensitive corporate data and thus it is critical for enterprise to protect mobile device security. In this paper, we discuss the current circumstances of mobile technology, services, different types of operating system, and the security challenges and various mobile network attacks. As the study carried on different security challenges and attacks, originate that mobile device should be used on trusted authorize websites & applications and don't trust unauthorized websites, third party applications and un-known source messages.

REFERENCES

[1] M. Kotadia, "Major smartphone worm by 2007," *Gartner Study*, June, 2005.

[2] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra, "A Survey on Security for Mobile Devices", 1553-877X/12, IEEE, 2012.

[3] Alexios Mylonas, Stelios Dritsas, Bill Tsoumas, Dimitris Gritzalis: "Smartphone security evaluation - the malware attack case" pp. 25-36, SciTePress, Spain, July 2011.

[4] Cassandra Beyer, "Mobile Security: A Literature Review", IJCA(0975-8887), vol 97-no.8, July 2014.

[5] Yong Wang, Karthik Vangury, Jason Nikolai, "MobileGuardian: A Security Policy Enforcement Framework for Mobile Devices", 978-1-4799-5158, IEEE, 2014.

[6] Ala Eshmawi &Suku Nair, "Smart Apllication Security: Survey of New Vector and Solutions", 978-1-4799-0792-2/13, IEEE, 2013.

[7] N. Boudriga, "Security of Mobile Communications". Taylor and Frances Group, 2010.

[8] Sabina Barakovic, Ena Kurtovic, Olja Bozanovic Anes, Jasmina Barakovic Husic, "Security Issuses in Wireless Networks: An Overview", 978-1-5090-2902-0/16, IEEE, 2016.

[9] Akhil Gupta, Rakesh Kumar Jha, "A Survey of 5G Network: Architecture and Emerging Technologies", 2169-3536, IEEE, 2015.

[10] Ting Zhao, Gang Zhang, Lei Zhang, "An Overview of Mobile Devices Security Issues and Countermeasures", 978-1-4799-7091-9/14, IEEE, 2014.

[11] R.Lakshman Naik, S.S.S.V.N Sarma, " A Framework for Mobile Cloud Computing", IJCNWMC, vol.3-2013.

[12] Dr. V. Harsha Shastri, V.Sreeprada, K.Anitha "Mobile Computing – challenges in Wireless LANs and Mobile Ad hoc Network". International Journal of Computer Trends and Technology (IJCTT) V42(3):141-145, December 2016.

[13] R Lakshman Naik, B Manjula, M Rajendra Prasad, "Dynamic Computation of the Application between Smart Mobile Device and Cloud Computing", IJCET-2014

[14] V Bapuji, SSVN Sharma, R Lakshman Naik, D Ramesh, B Manjula, "Quality of service for mobile Ad-hoc wireless networks", IJCSE, 2011, pp:1573-1577.

[15] Durga Puja, Raghav Mehra, BD Mazumdar "Context Provisioning for Mobile Service Ensembles". International Journal of Computer Trends and Technology (IJCTT) V37(2):46-54, July 2016.