Journal of Engineering and Applied Sciences 12 (Special Issue 5): 7014-7018, 2017
ISSN: 1816-949X

Mobile Device and Communication Security from Vulnerabilities, Malicious Attacks with its Solution

Vaibhav Gupta, Himanshu Singla, Ruhani and Poonam Nandal
Department of Computer Science and Engineering, Faculty of Engineering and Technology,
Manav Rachna International University, Faridabad, India

Abstract: Mobile security has become conspicuous in mobile computing including communication through mobile devices. Various users or businessmen's uses Smart phones to communicate. The Smart phones that are used as communication devices are compiled with the stack of sensitive information, hence, it is necessary to keep a check on them. The paramount focus of this research is on the notion of communication through mobile devices. Selected security risks have been discussed in this study that is analogous during communication through mobile or wireless devices. Various modes of communication like GPRS and VPN are also discussed with their limitations and advantages. Further, solution to the problem of Layer 2 Tunneling Protocol in VPN is proposed in this study which enhances the speed of the data transmitting through firewall.

Key words: Mobile security, communication, data, GPRS, VPN, protocol

INTRODUCTION

In modern era, mobile devices are acting as a heart for the communication system application. Communication through mobile device can be achieved with the aid of mobile computing sometimes also referred as nomadic computing which can be used as movable computing devices with mobile communication technologies. Mobile devices are the firmest rising user technology with world wide element sales predictable to escalate from 300 million in 2010 and 650 million in 2012. It brings an advantage of creating communication in remote areas through mobile devices. Mobile uses are always growing over era of time. In 2011 June, initially, people on normal expended additional time approximately 81 min every day using applications of mobile as compared to browsing the web which was approximately 74 min every day (Sujithra and Padmavathi, 2012).

Threats in mobile: The threats in mobile are referred to as any kind of malware that considers mainly PDA's, laptops and Smart phones. It can also act as Spyware that can steal the user data, information. Spyware threats or malware threats both can access user's private data without being noticed or can also make any malicious activity within the device's data. These types of mobile threats are divided into various kinds such as threats based on application, web, network and physical threats which are additionally discussed concisely. We have also given various types of threats in Fig. 1 and further, we will give in detail the various types mobile threats.

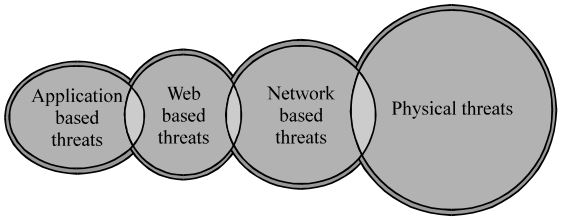

Fig. 1: Various types of threats

Threats based on applications: The applications from web that can be easily downloaded can cause numerous security threats on devices like mobile containing both hardware and software particularly designed to be malicious. Application based threats can be further divided into four categories. Malware, Spyware, vulnerable applications and privacy threats.

Web based threats: With increase in the use of internet through mobile devices, it can because web based threat the device get in touch or in connection to an open world of connection which take the devices to a vulnerable zone where device can be attacked or can be in danger zone easily. Now, this web based threats are divided into two categories as follows. Browser, exploits, drive by downloads.

Network based threats: Mobile devices support two kinds of networks that are cellular as well as local wireless networks. Network refers to a connection between devices or PDAs through wires, cables or via. wireless

Corresponding Author: Vaibhav Gupta, Department of Computer Science and Engineering,
Faculty of Engineering and Technology, Manav Rachna International University, Faridabad, India

modes. Network based threats can be divided into three categories. Network exploit, Wi-Fi sniffing, mobile network services.

Physical threats: As devices like mobile phone can be carried anywhere (portable) and are prepared for daily lives, its physical security is a major issue. Businessmen, security agencies or any user might contain important data within devices. Physical threats be like lost of devices or device got theft and also includes physical damage to the devices by falling or someone doing any harm to the device intentionally.

Sometimes attacker's just installs malware on the device by having access for few minutes on it rather than intercepting the messages once send. Once, these malware hits the mobile devices it can create destruction such as troublesome operations in mobile devices, collecting confidential information and having control on personal mobile device systems, this creates crashes in mobile devices.

MATERIALS AND METHODS

Transmission medium: Transmission that is something refers to the transmissions like point-to-multipoint or point-to-point. It has been widely known that for the purpose of telecommunication in the US, federal standard 1037C, the media based on transmission are categorized as guided, wireless (or unguided).

In this study, we are discussing about the modes of transmission used by mobile devices to communicate. Further, we are providing differences between the modes of transmissions:

Physical transmission medium in mobile devices: A physical transmission medium can be a material substance that is use to multiply that is to propagate waves. Transmission medium can also be defined as a technical tool that can communicate or guide the waves. Thus, it is found that an optical fiber or copper cable or electromagnetic waves or GPRS can be used as communication medium. The electromagnetic radiation can be transferred via. an optical medium, like optical fiber or via. twisted pair wires, dielectric slab waveguides.

Wireless transmission medium in mobile devices: Telecommunication through wireless transmission medium does not require any physical wires or any guided (bounded) medium to confine the path either for waves or for signals, we can also say the information or power is transferred among two or more than two points that are not consistent via. electrical conductor. In addition, the uses of radio wireless technology comprise garage door corkscrews, headsets, wireless computer mice and GPS units. Some rare methods that are also used for having a wireless communication brings the use of some other electromagnetic wireless technologies, like use of sound magnetic and electric fields or light (Coninx *et al*., 2003; Nash *et al*., 2005). Various applications of wireless transmission medium can be classified as follows:

Mobile telephones: These are one of the preeminent known amongst all the device examples of wireless technology, also called as mobile or cellular devices. These cellular devices were having more than 4.6 billion cellular subscriptions worldwide in 2010. All these devices use radio waves to deliver phone call services from signal-transmission towers to their mobile users.

Transfer of energy: The energy transfer is a process in which electrical energy is communicated power source to load which is electrical and is not having in-built power source. In general there are various advantages for wireless networking like receiving signals far from the source which provides the convenience by not having physical wires. Other than, this wireless networking also provides:

Mobility: With the rise in public wireless networks, individual can have access over the internet from being away from their working environment.

Ease of integration and convenience: This feature allows the users to have access over the network from any convenient location.

Expandability: Wireless networks provide the feature of expanding its client by any number whereas in wired network it makes the network typical. Wireless networking also has few pitfalls also signals of radio frequency transmissions are interrupted because of complex propagation effects that cannot controlled by network administrator and requirement of repeaters, routers and additional access points to increase the range of the signals increase the cost as well.

In Table 1, we have discussed properties of physical and wireless transmission in terms of their speed, physical network, expandability, attenuation, sound magnetic and dispersion. Wireless transmission (Chen and Kotz, 2000; Barnard *et al*., 2005) dominates physical transmission by having high speed without the use of wires. Its range can also be extended by using devices like routers (Gikas and Grant, 2013).

Table 1: Properties of physical and wireless transmission

Properties	Physical transmission	Wireless transmission
High speed	✘	✓
Need wires	✓	✘
Expandability	✘	✓
Attenuation	✓	✘
Sound magnetic	✘	✓
Dispersion	✓	✘

Wireless transmission methods: Wireless transmission is the kind of unguided media. Wireless communication involves having no physical link between two or more devices. Wireless signals propagate over in the air and is received by their supposed antennas. In numerous years, technology has elevated to the idea where many dissimilar forms of data is transmitted by means of wireless technology. There are many methods of wireless data transmission based on different technologies or techniques for transmitting data in the most effective and efficient method. Further, we are discussing about various methods of transmission.

RESULTS AND DISCUSSION

General packet radio service: One of the medium provided for the communication between mobile devices or wireless devices is GPRS, i.e., general packet radio service. GPRS tradition is classically charged based on the capacity of data transferred in comparison with circuit switched data which is paid per minute of connection time. The billing time is divided into one-third of a minute. The unit according to which billing is done by charging per megabyte. GPRS allows various users to share the service concurrently. The GPRS Network has brought the world towards Third Generation (3G) communication systems. GPRS optimize the use of radio services by using it only when the data is need to be sent. This network works on the basis of IP technology and is linked to public internet. With the aid of this feature GPRS is able to provide multiple or a variety of packet oriented multimedia applications (Zhang *et al*., 2011). The GPRS utilities are short message service and broadcasting, PTT (push to talk) through mobile data, point to point service, internet features for modern day devices, MMS.

Usability of GPRS: The extreme speed of GPRS linking was offered 2003 in a analog wired telephone network. It was about 30-40 kbps. The delay between the transfer of data is very high, it is about 600-700 m/sec and sometimes it reaches to one second. Certain operators provide the feature of performing up-gradations in network. This can lead to reduce the latency that is the time taken to transfer the data and increasing throughput speed.

Coding schemes and speeds: An important characteristic of data communication is to assure that data arrives and the data is unchanged. GPRS consist of 4 diverse coding schemes CS-1 to CS-4. The major difference between the 4 Coding schemes is the level of production or security it provides from transmission errors that they offer and keep a check such that maximum throughput can be obtained. The amount of BTS TDMA timeslots provided by the operator and encoding among them are the factors that affect the upload and download speed in GPRS.

Multiple access schemes: Frequency Division Duplex (FDD) and TDMA are the numerous access approaches that are used in GSM with GPRS. The packets have constant length according to the timeslot of GSM. FCFS (First Come First Serve) method is followed by the down link whereas the up-link follows a scheme that is nearly alike to reservation ALOHA (R-ALOHA). Meaning that slotted ALOHA (S-ALOHA) is used in enquires for reservation during the procedure of contention phase, after that the real data is transmitted via. dynamic TDMA with FCFS method.

Channel encoding: This process of channel encoding in GPRS consist of two step: First, for adding parity bytes cyclic code is used that is also referred or called as block check sequence. In Table 2, CS-1 to CS-4 are the coding schemes that specify the parity bits which were generated by cyclic code. CS-1 and CS-3 are the coding schemes in which, respectively input bit is transformed into two coded bits although, in CS-2 and CS-3 the desired code rate is achieved by puncturing the convolutional code where as in scheme CS-4 no use of convolutional code is applied (Holma and Toskala, 2004).

According to Table 2, it can be pragmatic that data rate is growing with the amount of slots we can also say that data rate is directly proportional to the quantity of slots. As we move from CS-1 to CS-2, according to the figures data rate is increased so as we move to higher coding schemes data rate increases due to improvement in security and less interruptions. In addition, there are two additional GSM technologies that distribute data services:

Circuit switched data and high circuit switched data. On the basis of sharing environment of GPRS it establishes a dedicated circuit that is generally billed per minute. Various applications like video calling which refers HSCSD, particularly when there is a big analogous that is continuous flow of data between the two sides. We have given some possible configuration of GPRS and CSDS in Table 3.

Table 2: Observed data rate according to the slots

Coding scheme	Max data rate for 1 Slot	Max data rate for 2 Slots	Max data rate for 8 Slots
CS-1	8.0	16.0	64.0
CS-2	12.0	24.0	96.0
CS-3	14.4	28.8	115.2
CS-4	20.0	40.0	160.0

Table 3: Some possible configurations of GPRS and CSDS (circuit switched data services)

Technology	Download	Upload (kbps)
CSD	9.6 (kbps)	9.5
HSCSD	43.2 (kbps)	14.4
GPRS	85.6 (kbps)	21.4
EDGE	236.8 (kbps)	59.3
3G	1-3 (Mbps)	28.0
4G	3-15 (Mbps)	41.0
5G (By 2020)	1(Gbps)	NA

The implementation of new applications and services through GPRS, security is anticipated as a vibrant factor because of the cause access over the wireless devices is less secure and they can be a fraud in the wireless connections so, this requires the network to have higher security risk factors to be encountered. At present, the wireless communication in mobile devices is held through passing the data via. GPRS while GPRS exchange its information through a public network. This can cause a security issue in the interval of transmission. It has become a clamorous problem needs to be sought out immediately. As GPRS exchanges its information or data through signaling it. Signaling exchange in GPRS is mainly based on the Signaling System 7 (SS7) technology that does not support any kind of security measure in the GPRS deployment. Likely, the GTP, i.e. [G (GPRS) Tunneling Protocol] which works for the communication between GSNs also does not support security. Hence, user's information and the data transferred using signals are exposed openly to multiple security threats. Further, communications in inter network (between diverse operators) are grounded on the public internet which permits IP Spoofing to any malicious third party who gets excess to it (Luo *et al*., 2011; McGraw and Morrisett, 2000).

VPN (Virtual Private Network): VPN refers to a virtual network extending a single private network along a public network like the internet, it seems as a private network link to the users. It allows users to exchange data with the help of networks like shared or public as if their devices are directly connected to the private network. Hence, applications executing along the VPN will help the user to have a better functionality, security and management if the private network. A VPN is established via. virtual point-to-point connection with the help of dedicated connections. A VPN also avail a feature a Wide Area Network (WAN). A VPN is also used to interconnect two comparable networks over a different middle network, for example, the 2 IPv6 networks over an IPv4 (Xenakis, 2008).

Limitations with VPN: One of the main issue or limitation with traditional VPNs is that they are not able to support broadcast domains they are point-to-points. The communication and networking which depends on Layer 2 and broadcast packets like net bios used in windows networking is not be entirely supported or work precisely as it would on actual LAN. VPN needs a brief description of issues related to network security and configuration, cautious installation that have adequate protection on internet. Also the presentation of an internet based VPN is not under the control of organizations, rather it depends on an ISP and their superiority of service. To overcome this issue Layer 2 Tunneling Protocol was organized. By using L2TP Protocol the issue related to domain based network is resolute.

Layer 2 Tunneling Protocol with proposed solution for high speed data transfer: Layer 2 Tunneling Protocol (L2TP) is an incorporation of earlier Microsoft Tunneling Protocol Point To Point (PPTP) and Cisco system's Layer 2 forwarding (Decker and Walke, 1993). Internet Engineering Task Force (IETF) told both the organization to work together by combining there protocols in the way to create a better protocol instead of competing each other. Hence, L2TP comes out as result. Basically, it researches on the structures of PPTP but runs with the faster transport protocol (UDP) and takes the help of IP sec to encrypt. The L2TP Access Concentrator (LAC) is known as the starting point of L2TP Protocol while the finish point is known as L2TP Network Server (LNS). LAC is initiates tunnel while the other one LNS is the server, it pauses for new tunnels. The traffic through the tunnel is bi-directional. But, there are 2 Faces of every coin L2TP is also having some pros and cons with it.

After mining about the methods of communication and its limitations, we have discussed main methods of communication like GPRS and VPN. VPN was brought to overcome the limitations of GPRS but as we have discussed in our research that everything have its pros and cons, therefore, we came to a limitation of VPN of not having security with higher data rate. It's important to have both security as well as speed. Security protects the data from vulnerability while speed is required to have a fast access over the network. There is a need to have a solution to overcome the problem of having only one feature at a time. In our research, we come with our proposal to use routers in the L2TP Protocol which will

help in solving the problem of low speed of data rate concurrently with a better security option. Routers will enhance the speed of data in the CPU and also increase the data rate, i.e., data transfer in between the firewalls.

CONCLUSION

In this study, we have discussed various methods of data transmission using major methods of communication like GPRS and VPN. We have also given the advantages and disadvantages of GPRS and VPN concluding that VPN is a better option rather than GPRS in context of data security, data rate and data interruption. Although, VPN is unable to handle a broadcast domain so to overcome this issue of broadcast domain Layer 2 Tunneling Protocol was suggested. Still, there is need to improve the data rate for which we have proposed a solution of using routers between the firewalls in Layer 2 Tunneling Protocol. In future, we will design architecture for enhancing the data rate in Layer 2 Tunneling Protocol.

ACKNOWLEDGEMENTS

Researchers would like to express the gratitude to Dr. Kiran Khatter, Research Mentor, Accendere Knowledge Management Services Pvt. Ltd. and other Research Mentors from Accendere KMS Pvt. Ltd. for their comments on earlier versions of the manuscript. Although, any errors are our own and should not tarnish the reputations of these esteemed persons.

REFERENCES

Barnard, L., J.S. Yi, J.A. Jacko and A. Sears, 2005. An empirical comparison of use-in-motion evaluation scenarios for mobile computing devices. Intl. J. Hum. Comput. Stud., 62: 487-520.

Chen, G. and D. Kotz, 2000. A survey of context-aware mobile computing research. Computer Science Technical Report No. TR2000-381, Dartmouth College, Hanover, NH., USA. http://www.cs.dartmouth.edu/reports/TR2000-381.pdf.

Coninx, K., K. Luyten, C. Vandervelpen, J.V.D. Bergh and B. Creemers, 2003. Dygimes: Dynamically generating interfaces for mobile computing devices and embedded systems. Proceedings of the 5th International Symposium on Mobile Human-Computer Interaction (HCI 2003), September 8-11, 2003, Springer, Udine, Italy, pp: 256-270.

Decker, P. and B. Walke, 1993. A general packet radio service proposed for GSM. GSM. Future Competitive Environ. Helsinki, Finland, 1993: 1-20.

Gikas, J. and M.M. Grant, 2013. Mobile computing devices in higher education: Student perspectives on learning with cellphones, smartphones and social media. Internet Higher Educ., 19: 18-26.

Holma, H. and A. Toskala, 2004. WCDMA for UMTS: Radio Access for Third Generation Mobile Communications. 3rd Edn., John Wiley and Sons, New York, USA., ISBN-13: 9780470870969, Pages: 478.

Luo, T., H. Hao, W. Du, Y. Wang and H. Yin, 2011. Attacks on webview in the android system. Proceedings of the 27th Annual Conference on Computer Security Applications, December 5-9, 2011, ACM, New York, USA., ISBN:978-1-4503-0672-0, pp: 343-352.

McGraw, G. and G. Morrisett, 2000. Attacking malicious code: A report to the infosec research council. IEEE Software, 17: 33-41.

Nash, D.C., T.L. Martin, D.S. Ha and M.S. Hsiao, 2005. Towards an intrusion detection system for battery exhaustion attacks on mobile computing devices. Proceedings of the Workshops on Pervasive Computing and Communications (PerCom 2005), March 8-12, 2005, IEEE, Kauai, Hawaii, USA., ISBN:0-7695-2300-5, pp: 141-145.

Sujithra, M. and G. Padmavathi, 2012. Mobile device security: A survey on mobile device threats, vulnerabilities and their defensive mechanism. Intl. J. Comput. Appl., 56: 24-24.

Xenakis, C., 2008. Security measures and weaknesses of the GPRS security architecture. IJ. Netw. Secur., 6: 158-169.

Zhang, X., F. Yang, Z. Liu, Z. Wang and K. Wang, 2011. Research and application of data security for mobile devices. Proceedings of the 4th IFIP-TC Conference on Computer and Computing Technologies in Agriculture (CCTA 2010), October 22-25, 2010, Springer, Nanchang, China, pp: 46-56.