Security Threats from Viruses in Cellular Communication

Md Bakash Ahamed
Department of Computer Science & Engineering,
Government College of Engineering & Textile Technology, Berhampore, Murshidabad,West Bengal, India.

Suchintya Sarkar
Department of Computer Science & Engineering,
Government College of Engineering & Textile Technology, Berhampore, Murshidabad,West Bengal, India.

Suvra Sarkar
Department of Computer Science & Engineering,
Camellia Institute of Engineering and Technology , Burdwan. West Bengal, India

Abstract - The Design of Security solutions of mobile communication is very challenging due to the poor user interface and limited processing capacity as well as complex network protocol. Still over a few years, smartphone has become very essential equipment for everyone. But some unscrupulous users try to bog down the smart phone or the whole mobile communication network system by spreading malicious codes in the form of Viruses or Worms or other malware which may result the huge disorder, operational vulnerability and leave the whole mobile phone networks to cripple ,ensuing a vast catastrophe. In this paper we want to alert the Cell phone or Smart phone users' community about how a cell phone or smartphones are prone to various malicious security attacks, online unsafe threats and then we would like to suggest some useful security solutions to combat with the menace.

Keywords: Network system, smartphones, Viruses, Security solutions.

I. INTRODUCTION

In modern digital environment, the smartphones have become essential communication medium for every human being. A very large number of mobile communication systems have been established and several service providers and equipment merchants are carrying to market a stable stream of new invention. According to the market forecast [9], about 30 million smart-phones are shipped in 2004 and about 3billions 4G smart-phones are shipped in between 2017 to 2019, after 3 years more than 2.5 billion of 5G smart-phones will be shipped. In the current year, smartphone users in our world reaches to 6.378 Billion, which renders to 80.8% of the world's total population. Since the powerfulness and the functionalities influences that of PC , the modern smart phone viruses could generate disorder and leave the whole telecom networks to cripple ensuing a immense catastrophe. The word functionality is frequently Interchange with security. A typical characteristic of security is that it provides no additional functionality to an application other than security itself. When application developers and users have to make a choice they therefore go for functionality rather than security, as a result the system becomes more prone to outside attacks from viruses or worms. We want to get thoughtfulness to the foreseeable security threats to modern smart phones from dangerous virus by this paper. Moreover, the inadequate magnitude and the poor user interface of the smartphone device stance specific difficulties for applying user pleasant applications in common and even more so for the smartphone security [8]. We first provide some useful background for the smart phones in part II. In part III we define about the smart phone virus and its works. Part IV deals with the upcoming connotations of the mobile virus threats in the world. In part V we converse certain solutions of the increasing mobile threat whereas we complete this paper in part VI.

II.SMART-PHONES

The very fast changing modern technology ,implementing robust Artificial Intelligence techniques transportability of mobile operating syetems,mobile communication networks, mobile devices and equipment's have enforced individual companies or organization to greatly depend on newly available functional products ,systems and infrastructure. With the smart-phones' or mobile devices, the two terms may be used alternatively, enlarged functionalities, they carry out many our daily activities, for example attending online classes, surfing the web, reservation of engagements, planning of the reminders, sharing data files, instant messaging, audio and video calling, mobile banking, controlling other devices such as Home theatres, running home electronic gadgets, controlling remote electronic devices and even more[18].

Generally, Smart Phones integrates the telecom and Internet services in a single device. It combines the portability of Cell-Phones with the computing and networking power of Personal Computers. Being the end point of both networks, Smart phones connect the Internet and the Telecom networks together. Since the smart phones are as powerful as old PCs, it becomes easy and low cost to introduce the Internet. The Operating Systems used in smart phones are Android, iOS (iPhone/iPad/iPod touch)[19], Palm OS , Symbian OS [9] Microsoft Smart-Phone OS, embedded Linux etc[7].

All of them have the following key features [8]:

- Access to cellular networks such as GSM/ CDMA/LTE/VOLTE
- Access to Internet with network interfaces like Wi-Fi, Bluetooth, GPRS, 802.11 and by means of TCP/IP protocol.
- Open APIs for applications, Data synchronization with the Personal Desktop Computer
- Multi-tasking feature to perform on multiple applications concurrently.

With almost all characteristics of PCs, the smart phones also create the common ground and opportunities for security breaches. Having full-fledged Operating Systems, they are also prone to virus and worm attacks. Moreover, having exposure to Internet, smart phones are becoming the target of attack by Internet spread able viruses and worms[22].

III. SMART PHONE VIRUS- NATURE OF ATTACKS

Given all the smartphones' operability, these devices are indeed vulnerable to online dangerous threats and are also very much prone to physical attacks because of their movability. Some of these security threats may include virus, malware explicitly intended for mobile devices i.e.the worms and spyware etc, illegal access, phishing, and burglary.

A virus threat is primarily an executable file which is envisioned to contaminate data on mobile phone devices.it has the capability to endure by duplicating itself and then it is also able to evade uncovering. Typically to evade finding, a virus cloaks itself as an authentic program which the operator would not usually suspicious to be a worm. Viruses are intended to corrupt or erase data on the hard disk's memory.

The Cell phone or smart phone viruses are designed to attack Cell phones and force them to malfunction. Nowadays, smart phones are at risk since, they are similar in functionality to actual personal computers what we are familiar with. Their vulnerability arises from the presence of an open operating system that, allowing for an Internet connection, exposes the phone to risks from such activities as sending of e-mail messages, exchange of MMS and WAP messages, as well as the use of accessories and tools. Communications that take place through Bluetooth or infrared connections become therefore potential vehicles for viruses. The most renowned viruses are 'Cabir' and 'Skulls' which corrupted thousands of smart phones[14].

On activating, a virus executes its malicious code for which it is designed in the background before the smartphone users comes to recognise about it's occurrence. Most attacks perpetrated to date and orchestrated by hackers exploit malware in the forms of games, screensavers and similar applications. So far, however, present cellular phone viruses have little impact to users, beyond the obvious hassle of phone malfunctioning[15]. The situation should not, however, be underestimated because it seems destined to change. Indeed, the malware authors only continue increasing their degree of menace in step with anti-virus professionals' ability to combat the threat. For the future, therefore, an increase of attacks designed to make the device completely inoperable is to be expected.

Maybe the most disturbing threat still remains that of the user's privacy: the cellular phone represents a de facto source of personal data with its phone numbers, messages, agenda and much more. The data can be erased, altered or filched. In a future scenario, therefore, it is important not to ignore the risk of attacks designed to seize valuable information, be it personal or professional.

Another disturbing phenomenon that has recently occupied a leading role among IT threats is spamming. Attackers can manipulate smart phone zombies to send junk or marketing messages through SMS. In the case of charge of

SMS is free, the owner may not even notice its bad behaviour. In the near future it seems apparent that cellular phones may become valid tools for the propagation of unwanted SMS and MMS messages[13]. The unwanted message may contain downloadable executable file and prompt to open it up. The moment user opens it, it gets infected. Mobile devices could therefore become the primary vehicle for the spreading of viruses aimed at infecting a large number of cellular phones that, once hit, would start sending unwanted spam SMS and MMS messages to all the numbers listed in the phone: all this while the unwitting user is charged for the costs of this fraud[11].

IV.SMARTPHONE DEVICE SECURITY THREATS

Here's the Smartphone device security are on the increase and what the prospect grasps[1][21].

4.1.Data Leakage-Mobile applications are frequently the basis of inadvertent data leakage. For sample, "riskware" , typically free applications originated in endorsed application stores that make advertisement .posture a genuine problem for Smartphone handlers who allow them broad approvals, but don't at all times check security. These are applications send individual—and hypothetically corporate data to a remote server, wherever it is excavated by advertisers, and occasionally, by cybercriminals. Data leakage can also occur through antagonistic enterprise-signed mobile applications where malware programs use distribution code innate to common mobile os like iOS and Android to move valued data across corporate networks without raising red flags.To avoid these glitches, only stretch apps the consents that they unconditionally requirement to correctly function[16].

4.2.Unsecured Wi-Fi-No one wants to burn over their cellular data when free wireless hot spots are accessible.—to be safe, use free unsecured Wi-Fi networks never use it to entrée confidential or personal amenities, like banking or credit card related information.

4.3.Network Spoofing-Network spoofing is when hackers create fake access points—networks that facet like Wi-Fi networks, but are actually traps—in high-traffic open locations such as coffee shops, libraries ,railway station and airports. Cybercriminals spring the access point's public names like "Free Airport Wi-Fi" or "Coffeehouse" to inspire handlers to join.In some cases, attackers necessitate handlers to generate an "account" to admittance these free services, ample with a password. As many handlers employ the similar email, password grouping for several services, hackers are then gifted to conciliation users' email, e-commerce and other protected information. As well as using carefulness when linking to any free Wi-Fi, never deliver private information.

4.4.Phishing Attacks-Because smartphone devices are always powered-on, they are the front lines of most phishing attack. Users are more at risk because they are habitually monitor their email in real-time, opening and reading emails when they are acknowledged. At no time click on unacquainted email links.

4.5.Spyware- In many cases, it's not malware from unidentified attackers that handlers should be concerned about, but somewhat spyware installed by spouses, colleagues or bosses to retain track of their locations and movement. Also known as stalkerware.many of these apps are intended to be loaded on the target's device without their consensus or awareness. A widespread antivirus and malware detection suite must use dedicated skimming methods for this type of program, which necessitates somewhat dissimilar handling than does other malware owing to how it gets onto your device and its determination.

*4.6.Broken Cryptography-a*ccording to Infosec Institute training materials, broken cryptography can occur when app designers practice weak encryption algorithms, or fail to correctly implement robust encryption. In the first case, designers might use familiar encryption algorithms notwithstanding their known vulnerabilities to accelerate the app development process. As an effect, any interested attacker can adventure the vulnerabilities to crack passwords increase access. In another instance, designers usage extremely secure algorithms, but leave other "back doors" open that boundary their efficacy. The responsibility is on designers and administrations to impose encryption standards before apps are installed.

*4.7. Improper Session Handling-t*o simplify ease-of-access for mobile device dealings, many apps utilize "tokens," which permit users to achieve multiple movements deprived of being involuntary to re-authenticate their identity. Improper session handling happens when apps accidentally share meeting tokens, for example with hateful actors, allowing them to imitate genuine users. Frequently this is the result of a session that leftovers open after the user has circumnavigated away from the app or website. For instance, if you logged into a corporation intranet site from your tablet and ignored to log out when you completed the job, by enduring exposed, a cybercriminal would be able to reconnoitre the website and other linked parts of your employer's network.

As said by Harvard Business Review (HBR), notwithstanding becoming a favoured target for hackers, mobile security is not decided in relation to network and computer security, reported that security expenditure was recurrently underfunded in relation to mobile app growth. As our dependence on mobile devices cultivates, so does the worth of data, and thus, the incentive for cybercriminals. As well as the mobile security threats we've just debated, be attentive for new threats attentive on the subsequent three key influence extents[9]:

4.8.SMiShing - Similar phishing scams, cybercriminals try to trick persons into transferring malware, ticking on malicious links or revealing delicate information. A SMiShing occurrence is thrown through text messages instead of email.
4.9. BYOD .-As corporate employees are settled high-level admission from the individual mobile network devices , the smartphone and, the tablets,phablets are efficaciously switching the PC or desktops for many professional accountabilities. So far, the different mobile devices don’t endorse the corresponding level of in-built security or controller as the organization-owned desktop computers they are substituting.
4.10. The Internet of Things (IoT) - With the number of types of smart devices—from RFID chips to thermostats and even kitchen appliances—rising so rapidly, they can’t always be watched by operators or antivirus resolutions. This constructs IoT device as an smart aim for hackers who use them as entry points to the superior high end network.

V. EFFECTIVE SOLUTIONS TO THE SMARTPHONE SECURITY

With the rapidly changing network demographics, the challenges round the mobile phone security are also varying, and specialists sense, it is the time to do away with incremental intelligent. With a mobile communication workforce, multifunctional multi-cloud networks, and enlarged hyper-connected networks, this unexpectedly swing to digital has lingering the space of security, putting running businesses, mobile phone users and data at a bigger risk than ever earlier. Making recent smartphone devices more secure is not a so very easy job, as there are very new vulnerabilities originated each day, it’s imperative to make assured that users are conscious of the distrustful operational activities that arise on their devices. The effective security can be convenient in all sides, at the Mobile set Kits, OS software used and at the Internet side or service provider. To guarantee a suitable level of security, it is necessary to protect the smart phones with essential anti-virus security package with an automatic updating facility that is sent straight to the smartphone or mobile devices. Smart phone or Mobile phone security solutions of the future will be multi-layered starting with preventive security incorporated in the OS, and with applications that retort more swiftly to new threats through spontaneous online updates. Mobile security solutions will therefore have to be modular and expandable in order to satisfy the needs of various types of mobile users. In compelling the platforms of phone security needed by mobile devices or smartphone handlers, the perilous facets will endure to be automation, ease of use and appropriateness of updating. The seamless invention thus will have to be automatic, easy to grip and skilled to compromise dependable and transparent defence. Users are obviously interested in the security of their mobile devices, but not in the technicalities. In other words: they want to be sure that in case of collision the airbag works, but they're not interested in how it works. Utmost latest effective ideologies of safe software development smudge to mobile applications as healthy. But certain key extents they must to effort on to acquire the finest outcomes.
Here are some effective practices may be endorsed to protect smartphone:

- Always use Secure Mobile phone, its OS, firmware, updates these when accessible to confirm the new security features and vital patches to evade Fresh loopholes might have exploited leaving the device exposed to threats .
- Always user should update the mobile phone with the latest application software. Installing apps from unknown developers should be avoided. Install application always from known and trusty site or store. Examination of the mobile Apps should be done sporadically whether working properly or not,
- Installing a trustworthy antivirus security application package with extra functionalities resolves assurance the mobile phone security example deleting phone data in case mobile device lost, chasing and blocking unidentified guests ,whether applications using or downloading are safe or not, apart from protection from dangerous virus, malware etc. Moreover, they offer to clear mobile phone browsing history and delete unnecessary cookies.
- The Personal Devices connected to a workplace network must be scanned systematically with the firewall, antivirus security system, and the anti-spam package or must not be permissible to link at all. Limitation of User Rights there in case of the public open networks
- Confirm first public open network or free open wi-fi is protected or not to protect against Wi-Fi hacking, make sure there is HTTPS linking to mobile network for secure surfing. Employ VPN connectivity whenever necessary to enable connection more secure.

- User should enforce a multi-factor authentications facility with strong password for further layer of security as soon as a operator logs into an application. Use strong passwords/biometrics such as fingerprint authenticators, make unauthorized access nearly impossible.
- Proper encryption methodology should be applied to mobile device to stop unlawful admission. Just find this feature on the smartphone device and give a user defined password for encryption properly. Encrypt Cache as well as to avert hacker to admission in to the cache.
- Implementation of Remote Wipe should be properly. Beware of suspicious emails, text messages, and hyperlinks in case read through smartphone. Minimal Application Permissions should be used, guarding sensitive information with a proper guarding mechanism to avoid online malicious threats. Hacker may steal very vital information by reverse-engineering programmes.
- Always Turn on smartphone device's auto-lock features to confirm others users cannot straightforwardly access it, Consultation with Security Experts is useful to acquire the essential security features of their application measured by third-party service providers
- Always turn off Bluetooth facility and Wi-Fi connection when not in use to avoid to unwanted unsecured connections, when not in use. Users should be careful to turn off the location tracking services features to neglect other outsiders to track your location history if there is no prerequisite of driving directions, daily traffic updates, and daily local weather update.
- Penetration Testing such as White box or black box testing may be used to check identified weaknesses in an application that an attacker might use and negotiation the security of the ultimate application. It comprises examination weak password strategy, unencrypted data, consents to third-party applications, no password expiry practice, etc. By re-forming the actions of a potential hacker, the security team controls whether any weakness exist in the application or not..
- Apply RASP security to defend an application against runtime threats by providing extra visibility into the unseen vulnerabilities. The RASP layer proactively analyses the inbound traffic and averts deceitful calls to operate within the mobile application. All inbound entreaties are examined by the RASP layer sitting in the middle of the mobile phone application and the external server.
- Code Obfuscation technique has become standard and is used to conceal program code from external threats. This is indeed effective methods to guard an application from the unknown hackers as it is challenging for hackers to appreciate.
- Some practical steps that will help you minimize the exposure of your mobile device to digital threats. Other effects to be considered such as turning off auto fill feature in case of web based form to protect personal data and log out of application– Subsequently using smart phone applications, particularly interconnected to one another, say Google platform, assurance that smart phone user logs off the application every time using it.

VI. CONCLUSION

We have seen that the aspects of mobile networks can make it both harder and easier to implement communication security as compared to Internet. Mobile devices usually have a poor user interface thereby creating problems for the usability of security. The network operators should control downloadable executable and thereby be able to filter out harmful executable, but it is questionable whether that will be accepted by the market. According to the experts at F-Secure research laboratories, in the future we are going to combat with a new breed of cellular device exploits, - for instance, Trojan Horses incorporated in games, screensavers and other applications generating unwanted charges, intrusions in reserved information filed in the memory of cellular phones, as well as data deleting or theft. Whereas isolated wiping and secure web surfing are decent practices to trail, the utmost serious practices for warranting mobile security are the mobile network security, OS architecture and firmware security and the application life cycle management. These are the underpinning pillars grounded on which a mobile phone device can be tested as secure or moderately unsecure. Whereas these good follows must be improved as the usage of mobile phone devices for economic and commercial dealings grow exponentially. Obviously, that will encompass many data being conveyed. The preeminent technique to defend a moble phone from the dangerous malicious viruses, malware or mobile date is to install anti-virus security suite that repeatedly updates itself. Os level as well as application level security suite generally aids as a remedy to resolve whatsoever vulnerabilities appear and not as a crucial objective in its own right, but it cannot afford too much defence against the very weak passwords and in case of a poorly designed mobile application. When 5G mobile communication network will become a prominent in the next 2-3 years, mobile phone security then will become imperceptible, so will the new challenges by means of augmented reality or may be the virtual reality. For an actual security infrastructure, it is imperative to make acquaint all the staffs about the security measures and go a step further and use AI/ML to pre-empt the problems that could arise and address them well. Although within the whole enterprise, checks the requirement to be ready to make sure that a breach in the enterprise network is under controlled and does not spread to outside untrusted network.

REFERENCES

[1] WAP Forum (2000a), WAP-199, WTLS (Wireless Transport Layer Security), Version 18-Feb-2000 URL: http://www.wapforum.org/what/technical.htm

[2] WAP Forum, "WAP Transport Layer End-to-end Security: Wireless Application Protocol", Approved Specification (Part of the July 2001 (WAP 2.0) conformance release): WAP 187, WAP Forum Ltd., URL: http://www.wapforum.org/, June 2001.

[3] W2Forum Research. Mon 7th Feb '05 URL: http://www.w2forum.com

[4] Microsoft Corporation. Windows Mobile-based Smart phones. http://www.microsoft.com/windowsmobile/smartphone/default.mspx.

[5] Moe Rehnema. Overview of the GSM System and Protocol Architecture . IEEE Communications Magazine, April 1993.

[6] The ISAAC research group. GSM Cloning. http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

[7] S.J.Vaughan-Nichlos. OS battle in smart-phone market. IEEE Computer, 36(6), 2003.

[8] ISO(1988), IS 7498-2. Basic Reference Model For Open System Interconnection-Part 2: Security Architecture, International Organization for Standardization.

[9] Hoshizawa, Y. (2002), Are JAVA-Enabled Mobile Phone Secured?, in U. Gattiker, ed., 'EICAR Conference Best Paper Proceedings', European Institute for Computer Anti-Virus Research(EICAR), pp. 141-151.

[10] Sajid Nabi Khan,Review paper on Android app security,Ikhlaq Ul Firdous, volume 7, p. 2277 – 128,April 2017

[11] Koyuncu, M., & Pusatli, T. (2019). Security Awareness Level of Smartphone Users: An Exploratory Case Study. Mobile Information Systems, 2019.https://doi.org/10.1155/2019/2786913

[12] Lefranc, S. & Naccache, D. (2002), 'Cut and paste attacks with Java', Cryptology ePrint Archive, Report 2002/010. http://eprint.iacr.org

[13] Netscape (1995), The SSL (Secure Socket Layer) 3.0 Protocol, Netscape Communication Corp.

[14] Krane, J. (2002), 'As Mobile devices get 'smarter', they become prone to viruses', SiliconValley.com – Mercury News, URL: http://siliconvalley.com/mld/siliconvalley/2833740.htm.

[15] Feher, Dr. Kamilo, Wireless Digital Communications, Modulation & Spread Spectrum Applications. Prentice Hall of India (PHI).

[16] Mariantonietta Noemi La Polla, A Survey on Security for Mobile Devices, IEEE Communications Surveys & Tutorials,January,2013

[17] Khan, J., Abbas, H., & Al-Muhtadi, J. (2015). Survey on Mobile User's Data Privacy Threats and Defense Mechanisms. Procedia Computer Science, 56, 376-383.

[18] Heisler, Y. (2016). Mobile internet usage surpasses desktop usage for the first time in history. Retrieved January 24, 2020, from https://bgr.com/2016/11/02/internet-usage-desktop-vsmobile.

[19] Platform Versions (2017, July). Android Developer. https://developer.android.com/about/dashboards/inde x.html

[20] Mobile Threat Report. (2016) McAfee https://www.mcafee.com/us/resources/reports/rpmobile-threat-report-2016.pdf

[21] Statista, Smartphones—Statistics & Facts, Statista, Hamburg, Germany,2020, https://www.statista.com/topics/840/smartphones/

[22] Milad Taleby Ahvanooey, Qianmu Li, Mahdi Rabbani, Ahmed Raza Rajput, A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks, ,26 Jan 2020, International Journal of Advanced Computer Science and Applications, 8(10), p.2017.