ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Survey on Security for Smartphone

[1]Dr. V.Sathiya Suntharam
[1]Department of Computer Science and Engineering, Galgotias University, Yamuna Expressway Greater Noida, Uttar Pradesh
[1] sathiya261@gmail.com

Abstract: Mobile phones were used exclusively for calls and messages many years ago. Mobile phone use has growing in a major way in the last decade. They have become more strong and advanced.They've come to call themselves smartphones. The smartphone has been highly popular among the human community thanks to its wide range of applications. The smartphone is gradually taking role of laptops and has begun to compete with computers for efficiently performing various user tasks. In addition to communication, the smartphone assists user activities by performing many tasks.The advances in technology in mobile connectivity services such as GPRS, GSM, 3G, 4G, Blue-tooth, WI-MAX and Wi-Fi have made mobile phones a necessary part of everyday lives. Mobile phones have also become smart, allowing users to perform on - the-go routine tasks.Author's contribution, in this paper is twofold. First, with a particular focus on smartphones, they review the threats, vulnerabilities, attacks and their solutions. Attacks are divided into two groups, namely old attacks and new attacks. With this classification, they aim to provide a quick and concise view of various attacks and possible smartphone enhancement solutions.

Keywords: Android, Anti-Virus, Blackberry, IOS, Mobile, Polymorphic, Security, Smartphones.

INTRODUCTION

Smartphones become as powerful as desktops and laptops. Smartphones ship with powerful graphics processors and multiple cores. They have robust GPS-containing sensor arrays, near field communications (NFC), Wi-Fi, Bluetooth and cellular capabilities. They're a vault for large amounts of personal financial services, social networking, and communication skills information. The modern smartphone's capabilities and information value make it an attractive target for miscreants about the Internet[1].The use of smartphones has risen significantly in recent years as smartphones provide users with multiple services such as phone calls, Internet services, data sharing, data storage, off-line gaming, online games, and some fun online / off-line applications.As smartphone offers vast resources, some problems such as security and privacy are also being saddled with. Since most smartphone operations are performed on the Internet, the security and security of data and information must be ensured[2].A pattern such as code password, PIN password, and face unlock can be used for mobile authentication. But these authentication mechanisms are not secured at high ratio because such steps could be breached with brute forcing and guessing.Critically, a lot of malware, viruses and Trojans were created based on

smartphone APIs (application program interface) and most of them look like secure software; some stable applications (Gmail, Twitter, etc.) collect user information such as bug-free geo-location with GPS service on smartphones.Multiple smartphone operating systems are present, including Android, IOS, Microsoft Window Phones, Symbian, and BlackBerry. Android is a commonly used mobile operating system with superior performance relative to other operating systems on smartphones. Android OS is architecturally based on the Linux operating system.The desktop OS and the smartphone variants of these operating systems, especially in user interfaces and system architecture, are very different. Using smartphones user can connect to Internet and communicate instantly with colleagues, partners and browse the worldwide web data / information[3].Today, mobile smartphones combine with other gadgets such as PDAs (personal data assistants), high-definition camera, music player, GPS navigation systems, and other storage and transmission devices.Also older mobile devices come

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

with 3 G and 4 G comparability; but in last decade, these devices have turned into mobile computers with the options of touch screen and desktop capabilities and can browse Internet using wireless network and third party applications[4].

GENERAL ARCHITECTURE OF SMARTPHONES

Smart devices combine mobile phones and networks with a rich networking and strong computing skills. A smartphone therefore has requisite computing platforms, operating systems, third-party software, and mobile hardware architecture modules.Unlike Android, apple operating system only works on devices like iPad, iPhone and iPod. The OS provides necessary infrastructure and interface to handle all operating systems and apps, as well as help to introduce new application to address a range of smartphone user needs[5].The apps allow mobile phone users to monitor their devices by interacting with operating system, enabling users to access and manage data communication interfaces and services through such interaction. The operating system, on the other hand, will access user data, and actually interact with other services and devices.Only hardware can be accessed directly in general operating system, but access to user data may result in user information being compromised and smartphone information may be mistreated by attackers just like computer attacks such as viruses, Trojans, etc. The most valued property of smartphones is the user data or information.As mentioned earlier, smartphones link via the Internet to several other electronic devices such as computers and even servers, in addition to communication. Usually the data without user knowledge is retrieved through applications infested with deceptive codes or programs[6].

STRUCTURE OF SMARTPHONES OPERATING SYSTEM

Android:Android is a smartphone, open source operating system built on the kernel of the Linux OS and released by Google. Android comprises four layers including the system kernel, libraries, Android Runtime, and Program.Application layer includes all Android applications such as email, SMS, instant messaging, browsers, contacts, and other applications whose names are longer than a several pages.According to authors all Android apps are recognized in and, application framework layer. Libraries layer is classified into two parts: The runtime library for Android and Android[7]. Android runtime blends Java Virtual Machine assets and Dalvik Server assets. Android library consists of the language C / C + +.

Windows Phone:Windows Phone Operating System was developed by Microsoft Corporation. Many devices for this OS including Nokia Lumia 800 and HTC Titan were built up in November 2011. After a year, Windows has become the fourth most commonly used smartphone operating system. Windows uses Android operating system as a model for stability.

IOS:The IOS is an operating system developed by Apple Inc for Apple devices. One famous example of this is the iPhone released in 2007. Now, iPhone is one of the biggest competitors in market shares for smartphones. Application of Apple phone will require computers running MAC OS. As with Android, new IOS has been developed for third parties to overcome platform capability limitations[8].

Nearly all smartphone operating systems provide mechanisms for users to improve the security of their devices through certain login mechanisms. More than 30 percent, however, on their phones, mobile phone users do not use the PIN. At the other hand, amount of highly valued information stored on the phone is growing rapidly, with mobile payment and money transfer software as well as business data on mobile devices becoming usable. The statistical data obtained from the sources were computed and shown in Table 1.

Table.1: Smartphone Estimation by OS 2014 Shipment and Market Share 2018

Vendor	2014 Shipment Values (Million)	2014 market % share	2018 Shipment values (Million)	2018 market % Share	Growth
Android	950.5	78.9 %	1321.1	76.0 %	10.7 %
IOS	179.5	14.9 %	249.6	14.4 %	10.2 %
Windows Phone	47.0	3.9 %	121.8	7.0 %	29.5 %
Black-Berry	11.9	1.0 %	5.3	0.3 %	-22%
Others	15.1	1.3 %	40.7	2.3 %	32.7 %
Total	1204.4	100.0 %	1738.5	100.0 %	11.5 %

SMARTPHONE PROBLEMS

Powerful hardware, sophisticated operating system, latest software, growing mobile capabilities and functionality are necessary, but an increase in current security threats on smartphones has become a prominent issue. Certain mobile features such as Internet large bandwidth accelerators, numerous peripheral interfaces that also disperse viruses across the network.Multi-connectivity is gaining considerable risk and making it easier to spread viruses that may be aggravating risks. Mobile device protection issues are close to the problems encountered in the personal computer world[9]. Threat means possible mobile security breakdowns.Given that the issues with smartphones can be divided into four categories: authentication data protection and safety, vulnerability and attacks.

Authentication in Smartphones:Authentication can be accomplished using the methods below. The first is to use what users know, like PINs or passwords. The second method is which frame consists of hardware, user data for operating system applications, and communication as protection.

To achieve the implicit authentication, a researcher suggested a multi-sensor based system for smartphones. The program ceaselessly studies the behavior patterns and environment of the user by allowing the user to use a phone without disrupting the activities of the user.Also, this method has the capacity to update user model. The experiment shows that this model's effectiveness only takes 10 seconds to run the model, and 20 seconds to detect unusual or fake requests. The accuracy achieved in this model can reach up to 90-95 per cent.

Another researcher suggested user verification system for monitoring the key users of mobile phones to dynamically distinguish authentic consumers from quacks. The authors used custom sample of 25 users to highlight the system proposed. That gives less than 2 percent of the fault rate after detection mode, and almost zero after PIN authentication is chosen.They also connected their approach to existing five state-of-the-art procedures to identify the simple keystroke for the user.

Data Protection and Privacy:Researchers addressed the issue of data protection from a user-centric perspective and explored the user's need for mobile systems to protect data. The authors discussed kinds of data that users want to protect; they also analyzed current user practices in data protection, and demonstrated how security requirements vary among different data types.We report the results of an exploratory usage analysis that interviewed 22 participants. Generally, it has been found that consumers want to protect the data on their devices, but consider it difficult to do so in practice, using the solutions available today.

A researcher presents the data protection problems from physical threats and the possibility of overcoming weak authentication. After interviews and survey studies, the user's data protection requirements are highlighted in that study.Finally, the author suggests that detection of unauthorized data access strategies does not cover adequate security although several vulnerabilities remain but these approaches are perfect for data traffics. Updating lock screen system to support authentication and device accessibility, and maintaining appropriate security, would improve user trust and smartphone health.

Vulnerabilities:Smartphones contain many multiple attacks and vulnerabilities. Smartphones have much vulnerability to build attacks that can lead to vulnerability, or be targeted by malicious attackers. Vulnerabilities of smartphones include: system failure / defects, insufficient application management, insecure wireless network and lack of user awareness.

a) System Fault / Defects:A smartphone cannot conceivably avoid both hardware and software faults. These defects disclose only after usage of the device. Sooner and later some defects may be detected / found. The software error can be easily corrected, but the hardware faults can cause anomalies and can be corrected by adjusting the hardware or modifying the design of the system.The attackers can exploit such flaws to initiate attacks on smartphones.

b) Insufficient Management of Apps: The smart devices ' most distinctive feature is their flexible APIs most of which are used to develop applications. Nonetheless, inadequate maintenance of the API is responsible for many infections with malicious code. Therefore mismanagement of the API is a major reason for malicious attacks on data. APIs are categorized into Open APIs, third party application development, and remote maintenance control APIs.Controlled APIs have specific

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

higher rights for device updating, file destruction, and retrieval of information. When attackers gain control of the APIs, they may easily launch attacks and take advantage of the API privileges[10].

c) Unsecure Wireless Network:They use Wi-Fi technology, Bluetooth, cellular network and GPS for connecting to any network or internet in wireless network. The packets on the network can be downloaded or fetched from any network computer hacker. So this is vulnerability and one can surmount it by using communication encryption / decryption technique.

Attacks of Smartphone:Attacks are normal in all computing devices and smart devices like smartphones, tablets etc. We will clarify significant attacks on smartphones in the coming row. The attacks are divided into two categories:

1) Old Attacks

a) Physical Attacks:Smartphones and tablets get misplaced or robbed quickly. Then, Sensitive data can be directly accessed and manipulated. Therefore, physical assaults damage drop or cover negative disposals.

b) Backdoor:Backdoor accepts intruders to develop a network connection while evading detection. Research has revealed many uses of backdoor target attacks. Backdoors result primarily from a controlled API system, bug, and revelation.Some smartphones, based on these vulnerabilities, come with insufficient authentications. In normal security, the attacker has access to the backdoor bypass.

c) Virus:Virus infects executable code, boot sectors and regular files, such as documents for word processing, PDF, etc. The virus replicates the file with consuming the system power. Viruses also provide a connection to an unknown source such as installer software without a user request. Researchers are introducing a virus detection and smartphone alerting system. This system detects viruses from the communication actions information. They study smart device's unusual behavior and develop a Smart-Siren system, and take result to show that the developed system effectively avoids viruses with reasonable overhead.

d) Trojan:Trojan is a mostly useful program but it has hidden malicious functionality. The aim is sneaked into the structure without the administration's knowledge.Smartphones are becoming increasingly complex and dominant in providing more functions; growing concerns about the opposite of security threats to smartphone users. Smartphones use the same software architecture as a personal computer, and are vulnerable to the same class of security hazards as viruses, Trojans and worms.

2) New Attacks:

a) Relay Attacks:This covers only potential mobile applications. APDU command interface / response network (GSM, UMTS, and Wi-Fi) relays security elements and method control relays. Attackers can use the protected victims as if they had their own physical possession. Additional resources may be obtained by relay application.Relay attacks are clear danger, and can use temporary contracts to circumvent security measures and encryption / decryption. In this work, the author's contributions include implementing practical demonstrations of the first relay attack using mobile platform technology from the NFC[11].

b) Cold Boot Attack:Smartphones and tablets get stolen or lost easily. This makes them vulnerable to low-grade memory attacks like cold-boot attacks using a bus, monitoring to keep an eye on the memory bus and DMA attacks.The article also discusses Sentry, a system that allows apps and operating system interfaces to store their code and data on the System-on-Chip (SoC) instead of the DRAM. They suggest use of an ARM-specific special mechanism designed specifically for embedded systems, but it is still in current mobile phones to protect applications and OS in conflict with a memory subsystem.

c) SMS Based Attack:Attacker can promote phishing links and distribute them via SMS attacks. An attacker can also use the text messages to feature vulnerabilities.Researchers are studying the security of SMS OTP (One-Time Password) system architecture and threats that pose a risk to internet and authorization learning authentication service. They resolve two basic OTP SMSerected on wireless networks, and when SMS OTP is intended and introduced they have completely dissimilar mobile devices.Which demonstrated why SMS

OTP system isn't safe again during this exertion? Their results are based on mechanisms proposed to ensure SMS OTP against collective attacks, and specifically against Trojan.

CONCLUSION

Smartphones are multifunctional mobile devices that typically contain of 3rd-party software that expand the device's functionality. The mobile malware is growing with the rapid development of smartphones prepared with many features like several communication links and sensors.The environment for smartphones is different from that of the PC. Similarly, approaches to avoid mobile infections and the dissemination of malicious code are distinct from PCs or other computing devices.Smartphones do not have adequate resources including power (battery) and processing unit. Increasing the smartphone's capabilities, attackers will exploit such features as various types of connections, sensors, services and the privacy of users.In this work, author discussed at first the current problems of authentication, data protection and security. They investigated vulnerabilities that can occur in smartphones and smartphone attacks. Second, they characterized recognized attacks that contradict smartphones, focusing on why attacks occur and what their effects on smartphones are.

REFERENCE

[1] L. Flynn and W. Klieber, “Smartphone Security,” *IEEE Pervasive Comput.*, 2015, doi: 10.1109/MPRV.2015.67.

[2] A. Das and H. U. Khan, “Security behaviors of smartphone users,” *Inf. Comput. Secur.*, 2016, doi: 10.1108/ICS-04-2015-0018.

[3] P. Faruki *et al.*, “Android security: A survey of issues, malware penetration, and defenses,” *IEEE Commun. Surv. Tutorials*, 2015, doi: 10.1109/COMST.2014.2386139.

[4] J. Joshi and C. Parekh, “Android smartphone vulnerabilities: A survey,” in *Proceedings - 2016 International Conference on Advances in Computing, Communication and Automation, ICACCA 2016*, 2016, doi: 10.1109/ICACCA.2016.7578857.

[5] P. Mach and Z. Becvar, “Mobile Edge Computing: A Survey on Architecture and Computation Offloading,” *IEEE Communications Surveys and Tutorials*. 2017, doi: 10.1109/COMST.2017.2682318.

[6] P. Gilski and J. Stefanski, “Android OS: A Review,” *TEM J.*, 2015.

[7] Tutorial Point, “Android Tutorial,” *Android, Tutor. Point*, 2014.

[8] T. Apple *et al.*, “Apple iOS,” *Apple*, 2012. .

[9] S. Farhan, M. Ali, M. Kamran, Q. Javaid, and S. Zhang, “A Survey on Security for Smartphone Device,” *Int. J. Adv. Comput. Sci. Appl.*, 2016, doi: 10.14569/ijacsa.2016.070426.

[10] C. Beyer, “Mobile Security: A Literature Review,” *Int. J. Comput. Appl.*, 2014, doi: 10.5120/17025-7315.

[11] A. Lima, B. Sousa, T. Cruz, and P. Simões, “Security for mobile device assets: A survey,” in *Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017*, 2017, pp. 227–236.

[11] Vishal Jain, Dr. S. V. A. V. Prasad, “Ontology Based Information Retrieval Model in Semantic Web: A Review”, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 4, Issue 8, August 2014, page no. 837 to 842 having ISSN No. 2277- 128X.

[12] Vishal Jain, Dr. S. V. A. V. Prasad, “Role of Ontology with Multi-Agent System in Cloud Computing”, International Journal of Sciences: Basic and Applied Research (IJSBAR), Jordan, Volume 15, No. 2, page no. 41 - 46, having ISSN No. 2307-4531.

[13] Vishal Jain, Gagandeep Singh Narula, "Improving Statistical Multimedia Information Retrieval (MIR) Model by using Ontology and Various Information Retrieval (IR) Approaches", International Journal of

Computer Applications 94(2):27-30, May 2014 having ISSN No. 0975-8887

[14] R.Santhya, S.Latha, Prof.S.Balamurugan , S.Charanyaa“ Investigations on Methods Developed for Effective Discovery of Functional Dependencies,”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015,

[15] T.Kowshiga, T.Saranya , T.Jayasudha , Prof.M.Sowmiya and Prof.S.Balamurugan“ Developing a Blueprint for Preserving Privacy of Electronic Health Records using Categorical Attributes,”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015.

[16] P. Lavanya, R. Meena, R. Vijayalakshmi, Prof. M. Sowmiya, Prof. S. Balamurugan , “ A Novel Object Oriented Perspective Design for Automated BookBank Management System”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Issue 2, February 2015.