ISSN:0975-9646

A Survey on Malware Attacks on Smartphones

Kireet .M[#1], Dr.Meda Sreenivasa Rao[*2]

[#]*CSE Dept ,Research scholar ,lecturer in JNTUH,HYDERABAD,INDIA*
[*] *CSE Dept ,Professor ,JNTUHSIT, HYDERABAD,INDIA*

Abstract—**Today, smartphone has become a part of our everyday lives since they enable us to access variety of services in time . At present , the usage of these mobile services has significantly increased due to the different forms of connectivity provided by smartphones, such as GPRS, Bluetooth and Wi-Fi. At the same time , the number of vulnerabilities exploiting these services and communication channels have increased as well. This made malware writers to choose smartphone as ideal target .This paper surveys the state of the art on threats, vulnerabili-ties and security solutions over the period recent period, by focusing on high-level attacks, such those to user applications. We group existing approaches aimed at protecting mobile devices against these classes of attacks into different categories, based upon the detection principles, architectures, collected data and operating systems, especially focusing on IDS-based models and tools. With this categorization we aim to provide an easy and concise view of the underlying model adopted by each approach.**

Index Terms— **Malware ,Intrusion Detection, Mobile Malware.**

I. INTRODUCTION

At present the Smartphones provide lots of the connectivity options, such as IEEE 802.11, Bluetooth, GSM, GPRS, UMTS, and HSPA. This allowed attackers to exploit just a single vulnerability to attack a large number of different kinds of devices by causing major security outbreaks.At first attackers relied on various scams which are delivered by email spams..By the enhancement of technology webbrowsers,email clients and custom applications became standard on smartphones,attackers started to exploit vulnerabilities beyond traditional e-mail and phishing attacks.

The main vector of mobile attacks is SMS spam which is unwanted messages.Unlike emails where the messages sent in the form of SPAM are unread the SMS spam is easiest way to attack where the victim will almost open or read every SMS that has come to his smartphone.The majority of the attacks in smartphones use social engineering tactics to convince the user to install or subscribe attacker controlled service.

A large percentage of attacks depends on convincing the user to join various dating portals,asking the user to participate in surveys to win the prizes.Once the user joins these portals or perform any surveys the victim will be in contact with a bot which performs malicious activities.

By gaining huge popularity android is the major platform for the attackers to introduce their malicious activities into their smartphones. it offers the third party application which can be downloaded and installed from Googleplay which is making the malware writers much easy to introduce their malicious activities into the smartphones.These malwares performs the various activities behind the scene which steals the sensitive information of the users.

In this paper current malware attacks on smartphones and detection methods are reviewed. Malware, short for malicious software, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency.

II REASONS FOR WHY SMARTPHONES ARE VULNERABLE

1.FirstlyMost of the users store their personal data in smartphones.They perform financial transactions,online banking transactions using smartphones.Attackers can have substantial financial gain from such sensitive data.

2.Secondly most of the smartphones use android platform.As android is open source kernel,malware writers can gain deeper understanding of the mobile platform

3.Third,most of the users view that smartphones are just used for entertainment and communication.They view that smartphones are handheld computers and not sensitive ,as a result no attention is paid on security measures.

III VARIOUS TYPES OF MALWARE ATTACKS ON SMARTPHONE'S

Phishing Attacks –The details such as user credentials ,creditcard numbers,account details are collected by using apps,emails,or SMS ,which seem to be genuine

Spyware Attacks – By using these type of attacks user's various information stored in their infected smartphones are exracted.

Surveillance Attacks – By making use of the built-in-sensors specific user is under survelliance by his/her infected smartphone.

Diallerware attacks - Using the malware that makes hidden calls to premium numbers or SMS services user's money is stolen.

Financial Malware attacks – By performing Man in the middle attacks on financial applications stealing user's credentials form the smart phones.

Worm-based attacks – Without user intervention through an existing network worm duplicates itself typically propogating from one device to another device

Botnets –Hackers try to monitor remotely b**y S**et of Zombie devices that are infected by malware.

III Methodologies Of The Attacks

The distinct methodologies to perform attacks against smartphones are categorized using the following classes:

- wireless;
- break-in;
- infrastructure-based;
- worm-based;
- botnet;
- user-based.

1)Wireless Attacks. To extract confidential information, such as usernames and passwords the most common attack is eavesdropping on wireless transmissions. Wireless attacks can use the unique hardware identification (e.g., wireless LAN MAC address) for tracking or profiling the owner of the device. Malware often exploits Bluetooth as a medium to speed up its propagation

2) Break-in Attacks*:* Uses buffer overflows or format string vulnerabilities to perform further attacks.i.e these Break-in attacks enable the attacker to gain control over the targeted device by exploiting either programming errors.

3) Infrastructure-based Attacks*:* Attacks done by using the basic services provided by the infrastructure which are essential for smart-phone functionalities, such as placing/receiving calls, SMS and e-mail services.

4)Worm-based Attacks :Worms can be easily spread by just one click to infect smartphones in any part of the world. The main features that character-ize attacks based upon worms are:Transmission channel, spreading parameters, user mobility models.

5)Botnet :Botnet forms a collection of zombie devices that are infected by malware of which these devices are remotely monitored.

6)User based Attacks : Most of the todays mobile malware are not of technical nature but just tricking the user into overriding technical security mechanisms like social engineering attaks .

IV Major Aims Of The Attacks

The major aim of attacks done by using malwares by the hackers are

1.**Privacy**: Major aim is to corrupt the integrity and confidentiality. Due to their small dimensions, smartphones can be stolen or lost more often than laptop computers., it may be possible that someone installs a spyware on the phone; someone can read personal data, as contact list or messages *2.*

2.Sniffing: These type of attacks based upon the use of sensors, e.g. microphone, camera, GPS receiver. These sensors enable a variety of new applications but they can also seriously compromise users' privacy.By compromising the smartphone attacker tries to access the data stored in the device and uses sensors to sniff and record all of the user actions.

3.**Denial-of-Service**: By using DOS attack attacker denies availability of a service or a device. DoS attacks against smartphones are mostly due to strong connec-tivity and reduced capabilities: due to the limited hardware, attacking a smartphone can be accomplished with a small the attackers.

4. ***Overbilling:*** These type of attacks charge additional fees to the victim's account and may transfer these extra fees from the victims to the attackers. Since many wireless services are regulated by pay-per-use contracts, these attacks are very specific to wireless smartphones

V Defence Methods For Attacks On Smartphones

Intrusion Detection Systems

Intrusion detection systems can be based upon two approaches:

1) *prevention-based*: Intrusion detection systems have to be running online and in real-time using cryptographic algorithms, digital signatures, hash functions, important properties such as confidentiality, authentication or integrity can be assured.
2) *detection-based* approaches: To effectively identify the malicious activities IDSes serve as a first line of defense .

Furthermore, there are two main types of detection:

1) *anomaly-based* This can also be called as behavior based detection or anamoly based detection where comparsion of normal behavior with “real” one is done.;
2) *signature-based* This *can also be called* as misue-based detection ,detection by appearance,knowledge based. detection based upon patterns of well-known attacks

Future risks associated with a smartphone include:

- data leakage resulting from device loss or theft;
- unintentional disclosure of data;
- attacks on decommissioned devices;
- phishing attacks;
- spyware attacks;
- network spoofing attacks;
- surveillance attacks;
- network congestion attacks;
- financial malware attacks;

In the following, we partition existing IDS solutions using these features:

- *detection principles*:
  – anomaly detection:
  □ machine learning;
  □ power consumption.
  – signature-based:
  □ automatically-defined;
  □ manually.
- *architecture*:
  – distributed;
  – local.
- *reaction*:
  – active;
  – passive.
- *collected data*:
  – system calls;
  – CPU, RAM;
  – keystrokes;
  – SMS, MMS.
- *OS*:
  – Symbian;
  – Android;
  – Windows Mobile
  -Apple iOS.

CONCLUSION :

This paper shows the types of malware attacks on smartphones,methodologies of attacks,major aim of different types of attacks,Present detection methods for attacks on the smartphones.By this analysis it can be said that more attention to be focused on how to collect the data of emerging malware systematically as they are usally hidden in apps distributed by the third party markets.Therefore novel approaches are needed for the discovery of new malware.

REFERENCES:

[1] L. Aouad, A. Mosquera, S. Grzonkowski, and D. Morss, “SMS spam:A holistic analysis,” in *Proc. 11th Int. Conf. Security and Cryptography,SECRYPT*, Vienna, Austria, Aug. 2014.

[2] GSM Association, *IMEI Allocation and Approval Guidelines*, Version6.0, 2011-07-27.

[3] Android WebView exploit, CVE-2012-6636. [Online]. Available:http://www.cve.mitre.org/cgibin/cvename.cgi?name=2012-6636

[4] M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, and V.Shmatikov, “The most dangerous code in the world: Validating SSL certificatesin non-browser software,” in *Proc. 2012 ACM Conf. Computerand Communications Security (CCS’12)*, pp. 38–49.

[5] D. Guo, A. Sui, and T. Guo, “A Behavior Analysis Based Mobile Malware Defense System,” *Proc. ICSPCS*, pp. 1–6, 2012.

[6] G. Hogben and M. Dekker, “Smartphones: Information Security Risks, Opportunities and Recommendations for Users,” Dec. 10, 2010, https://enisa.europa.eu/smartphonesecurity

[7] S.-H. Seoa *et al.*, “Detecting Mobile Malware Threats to Homeland Security Through Static Analysis,” *J. Network and Computer Applications*, vol. 38, Feb. 2014, pp. 43–53.

[8] Landesman M. The World’s Largest Security Analysis of Real-World Web Traffic, Annual Global Threat Report, ScanSafe STAT. Available at: http://www.scansafe.com/downloads/gtr/2009_AGTR.pdf (Accessed 16 Feb. 2011).

[9] Ray B. Home Office discusses thief-proof phones. Available at: http://www.theregister. co.uk/2007/05/25/home_office_phone_crime (Accessed 16 Feb. 2011).

[10]. Kruegel C, Valeur F, Vigna G. Intrusion Detection and Correlation: Challenges and Solutions. Book chapter Computer security and Intrusion Detection, Springer, 2005.

[11]. Singh KK. Hybrid Profiling Strategy for Intrusion Detection, Department of Computer Science University of British Columbia, 2004.

[12] Hammersland R. ROC in Assessing IDS Quality, Norwegian Information Security, Gjovik University College, 2007.

[13] Moreau Y, Verrelst H, Vandewalle J. Detection of mobile phone fraud using supervised neural networks: A first prototype, Procee[ings of the 7th international Conference on Artificial Neural Networks (ICANN’97) 1997; 1065-1070.

[14] Buschkes D, Kesdogan R, Reichl P. How to Increase Security in Mobile Networks by Anomaly Detection, Proceedings of the Computer Security Applications Conference, Phoenix, December. 1998; 3-12.

[15] Boukerche A, Notare MSMA. Behavior-Based Intrusion Detection in Mobile Phone Systems. Journal of Parallel and Distributed Computing 2002; 62(9): 1476-1490.

[16] Hollm´en J. User profiling and classification for fraud detection in mobile communications networks, PhD Thesis, Helsinki University of Technology, 2000.

[17] Burge P, Shawe-Tylor J. An unsupervised neural network approach profiling the behavior of mobile phone users for use in fraud detection.