ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Mobile Virus Prevention Techniques: A Survey Perspective

R.Dhaya[1], M.Poongodi[2]

Faculty, Department of CSE, Velammal Engineering College, Anna University, India[1]

Student, Department of CSE, Velammal Engineering College, Anna University, India[2]

ABSTRACT: As mobile phones has become more commonly used gadget. Proportionately it has become increasingly difficult to secure them against attacks in the form of viruses or other malwares. Malwares are malevolent Software's. That can disrupt the operation as well as function of the mobile phones like smart phones, Tablets, Personal Digital Assistant and transmit or modify user data .Mobile virus can cause system failure, wasting memory resources, corrupting data and also increasing the charges of maintenance cost. So Mobile Security is has become very important one in mobile computing. This paper discusses the several techniques of malware detection or preventions such as Signature based detection, Behavior based detection, Support Vector Machine, N-gram etc, to detect the malwares such as virus, worms etc.

KEYWORDS- Malware, Signature based detection, SVM, N-gram

I. INTRODUCTION

While comparing to the hand-held devices with computers, mobile devices like smart phones, tablets etc, are very intellectual and difficult in its functionality. Mobile phones are used in many activities like Net banking, on line shopping, Education, Business etc. Because of this high-end facilities, mobile phones are very prominent than computers. The outcome of the mobile phone usage is to escalate the dishonest people who would like to take an advantage of these actions for unlawful gains. Malware is a very big danger in the present technology driven world. Mobile Malware is an acronym of "malicious software" - particularly built to target mobile devices such as smart phones, tablets to harm the devices. Malware has the capability to contaminate other system files, executable files and corrupts the data. Malware is a program aimed to damage the system, such accessing location information via Global Positioning System(GPS), address book, transmitting data on the network, sending SMS that are charged, etc. several types of malwares are available such as Viruses , Worms, Trojan etc. Many of the mobile viruses come into the mobile devices while downloading the applications through an internet. Due to these reasons mobile security is a vital one. Malware can gain the access to an information system ,record and send data from the system to a third party without user's knowledge, conceal the information has been compromised, disable the security measures, damage the system or affect the system integrity. Malware is able to compromise information system due to combinations of factors that include insecure operating system design and related vulnerabilities. Malware works by running or installing itself on an information system manually or automatically.

II. OVERVIEW OF MOBILE MALWARES

Malware is a malicious software program that are designed to damage the hand-held devices such as smart phones, tablets and Personal Digital Assistant(PDAs).There are several types of malwares available such as mobile phone virus, worms, trojan, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

2.1 Mobile Virus

A mobile phone virus is a malicious software program that targets cellular phones and other wireless PDAs. Once phone is infected, it can become a source for spreading the virus by sending texts and emails to other vulnerable devices. These texts and emails can lead other users to open or download the virus. Mobile phone viruses can also come in the form of malware that spreads through downloaded applications. Virus is a program that inserts itself into one or more files and then performs some action for example cabir virus running symbian operating system.

2.2 Worms

Worm is a program that reproduce itself and spread to other devices in order to the operating system of interaction for execution. Worms may contain harmful and misleading instructions. Worms can spread from removable media to computers (Compact Disks(CD), Universal Serial Bus(USB sticks, etc), Spread between mobile phones (via SMS or MMS messages over the telecommunications networks, or via Bluetooth wireless networks), Spread between accounts on a social networking site such as Face book or Twitter. An SMS-worm is a type of worm that distributes copies of itself to new victims. It may be able to automatically send a copy of itself to every contact listed in the mobile phone's contact list.

2.3 Trojan Horse

Trojans are not able to self replicate. Trojans are malicious programs that perform actions that have not been authorized by the user. Trojan horse always requires user interaction to be activated. This kind of virus is usually inserted into seemingly attractive and non malicious executable files or applications that are downloaded to the device and executed by the user. Once activated , the malware can serious damage by infecting and deactivating other applications or the phone itself, rendering it paralyzed after a certain period of time or certain number of operations.

2.4 Spyware

Spyware is type of malware that aids in gathering information about a person or an organization without their knowledge. This malware poses a threat to mobile devices by collecting, monitoring, using and spreading user's personal or sensitive information without the user's consent and knowledge The activities recorded by the spyware is to gather email address, credit card number, key pressed by the user etc.

2.5 Adware

Adware is a software and it contains a commercial advertisement like games, desktop toolbars. It is a web based virus and collects the web browser especially in pop ups.

2.6 Rootkit

Rootkits are designed to take control of an infected mobile devices by obtaining administrator access of another device. The name came from UNIX(Uniplexed Information Computing System) operating system.

III. BROADCASTING VECTORS OF MALWARES

The malware broadcasting vectors of to the electronic methods by which is transmitted to the information systems, platforms, devices it seeks to infect. Examples of broadcasting vectors include the World Wide Web(WWW),SMS,MMS,BT etc. The following vectors are commonly used to broadcast the viruses/malwares,

- Short Message Service(SMS): SMS is the transmission of short text messages to and from mobile phone, fax machine and Internet Protocol(IP) address. Message must be no longer than 160 alphanumeric characters and contain no messages.SMS are supported by GSM, Time Division Multiple Access(TDMA),Code Division Multiple Access(CDMA) based mobile phones currently in use. Once a message is sent, it is received by Short Messaging Service Centre(SMSC) which must direct it to the appropriate mobile device. SMSC send a SMS request to the Home Location Register(HLR) to find the roaming customer. Once the HLR receives request, it will respond to the SMSC with the customer status. A same series of steps are followed to reach the message in receiver's side.
- Multimedia Messaging Service(MMS): MMS is developed by Third Generation Partnership Project(3GPP) that allows users to exchange multimedia communications between capable mobile phones and other devices.MMS defines a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

way to send and receive, almost instantaneously wireless messages that include images, audio and video clips in addition to the text. It will support the transmission of streaming video.

- Bluetooth(BT): Bluetooth is a technology which are local area networks with a very limited coverage and low cost without need of the infrastructure. Different type of network is needed to connect different small devices in close proximity without expensive wiring or need of wireless infrastructure. the advantage is , it consumes low power, low cost it and it is used in mobile phones, laptops, tablets and PDAs.
- Internet Downloads: The mobile user downloads an infected file to the phone by the way of user's mobile internet connection or Personal Computer(PC)'s net connection. It may disguised as attachments like images, greeting cards, audio or video files and add on-sites. It can be spread through spreading and downloading the applications.

IV. DIFFERENT TECHNIQUES TO FIND MOBILE MALWARES

4.1 Malware Detection Methods

There are many types of techniques are available to detect mobile malwares. There are some common methods to find the malwares.

- Signature Based Detection:Most of the commercial antivirus companies used a signature based detection methods to identify malwares. Signature is the binary of pattern of the machine code of a particular virus. It checks the content of the file dictionary of malware signatures. This method needs the huge database to store the malware signatures. It fails to identify an unknown malwares because a new malware may not contain a known signature of malwares. It is vulnerable to simple obfuscation, polymorphic and packing techniques.
- Behavior Based Detection:Behavior based detection mechanism monitors the run time behavior of the mobile application and compares the malicious and/or normal behavior profiles to detect the malwares. It explains the what behavior should be monitored, how to monitor and how to collect the behavior varies. It is flexible to simple obfuscation, polymorphic and packing techniques. The malware is analyzed in three ways. They are followed by,
- Static analysis: Static analysis is the process of analyzing the code without executing the file and it reveals the source code. Static code analysis is the process of detecting errors and defects in software's source code. It can be viewed as an automated review process.
- Dynamic analysis : Dynamic analysis is the process of executing the file and observing its behaviors, interaction and effects on the devices. It is the testing and evaluation of a program by executing data in real time. The objective is to find an errors in a program while it is running rather than repeatedly examining code offline.
- Hybrid analysis: Hybrid based analysis is a combination of both static and dynamic analysis. This method is used to overcome the limitation of both static and dynamic analysis. The figure 1 shows various types of malware detection techniques.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

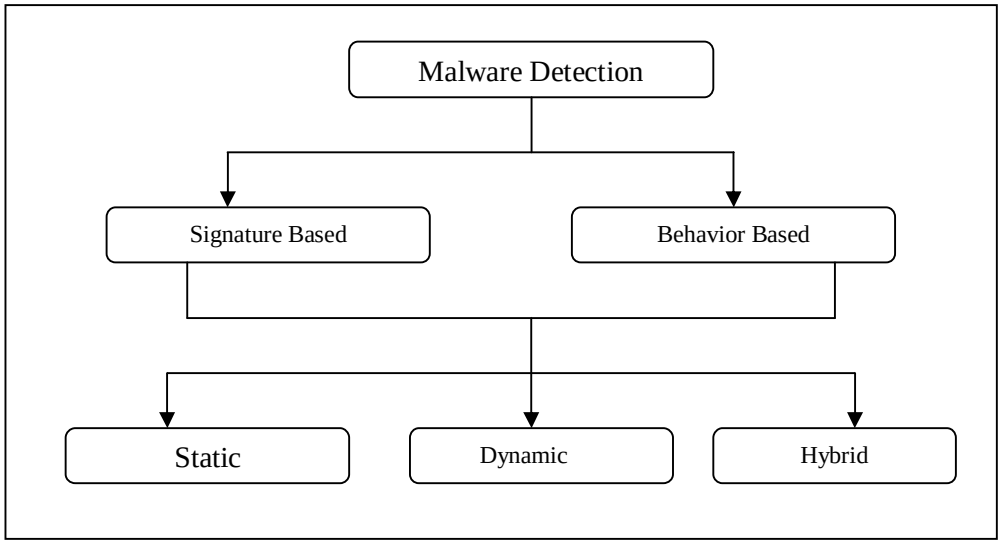

Figure 1: various types of malware detection techniques

4.2 BASED ON TYPOLOGY

There are three types of malware detection and prevention are available based on typology. They are followed by,
Device Based Detection Typology: In device based technology, mobile detection mechanism are completely constructed on the device itself. This method is restricted by resource constraints because mobile handsets have a limited resources in terms of battery power, storage capacity and computational methods.
Infrastructure Based Detection Technology : In this method collects the information based on infrastructure components and organized in hierarchical manner. Computationally very expensive to implement this system.

Hybrid Typology : This method is combination of both device based and infrastructure based detection mechanism. In this, part of the detection mechanism runs on the device and another part of the detection mechanism operates on the infrastructure. The figure 2 shows various types of malware detection based on typologies.

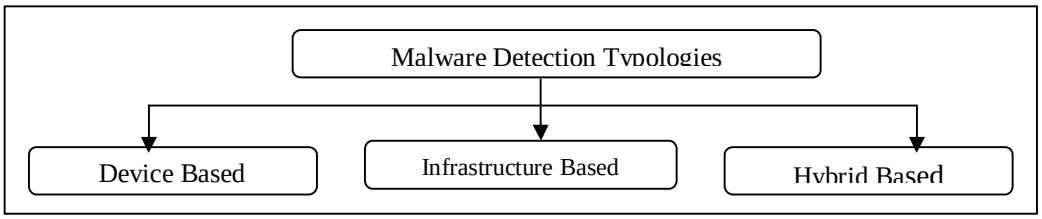

Fig 4.2 Malware detection types based typologies

Figure 2: types of malware detection based on typologies.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4.3 Agent Based Malware Modeling (AMM)

Agent Based Modeling is a used to examine the malware utilizing SMS/MMS/BT vulnerabilities on the mobile phone devices. AMM uses a centralized agent(collection of entities) that has the capability of autonomous decision making. The agents may be mobile phones, PDAS, Service centre and gateways. Agents are grouped in a hierarchical manner.AMM simulator uses several parameters to develop the malware propagation. Exchanging the messages between agents through service models.AMM model uses various algorithm for malware detection and it can be implemented based on hierarchy. This method is computationally very expensive. Once the centralized agents, the entire system will affect.

4.4 Support Vector Machine(SVM)

Signature based detection method fails to detect a new malwares. Due to that problem, Behavior based detection mechanism was proposed to identify the new malwares with the help of machine learning algorithm named Support Vector Machine(SVM). Behavior based detection monitors the behavior of an application and compares the malicious and/or normal behavior profiles to detect the malwares. Support vector machines are supervised learning model with associated learning algorithms that analyze data and recognize patterns used for classification and regression analysis. SVM takes a set of input data and predicts, for each given input which of two possible classes forms the output. Giving a set of training examples ,each marked as belonging to one of two categories ,an SVM training algorithm builds a model that assigns new examples into one category or other. It is used to analyze the data and used to train the classifier to classify from the malicious and non malicious data. Behavioral detection framework uses the behavior signatures that describes the behavior of an applications in the entire set and monitors it and compares the malicious and benign code. It provides the high detection rate in malware detection.

4.5 Data Mining

Signature based detection method fails to identify a new malwares, a proposed method is named data mining methods which is used to detect a unnoticed malwares. The goal of the data mining process is extracting to extract information from a data set and transform it into an understandable structure for further use. Data mining methods are used to detect the patterns in large amount of data and to detect the future instances in similar data with the help of these patterns. Naive bayes algorithm is used to classify the malicious code(MC) and begin code(BC) and detect new malwares. A naive bayes classifier is a simple probabilistic classifier based on applying bayes theorem with strong independence assumptions. Probability model would be independent model.P(C|F1,F2,F3.....FN) over a dependent class variable C with small number of outcomes or classes, conditional on several feature variables F1 through FN. The problem is that if the number of features N is large or when a when a feature can take on a large number of values, then basing such a model on probability tables is infeasible.

4.6 N-Gram analysis

N-gram model is a type of probabilistic language model for predicting the next item in such a sequence in the form of a (n-1) order markov model. N-gram models are now widely used in probability, communication theory, computational linguistics and data compression. It has the capability to capture the inherent features of the given input data. It is used to extract the most frequent N-gram signatures in the given database. When a new code is analyzed , it can be classified as MC/BC based on the category it matches the most. An advantages of N-gram models are relatively simplicity and ability to scale up by simply increasing n-model can be used to store more context with well understand space time trade off, enabling small experiments to scale up very efficiently.

V. CONCLUSION

This paper focuses on mobile malwares and impacts of the malwares on the mobile phones. This paper have been discussed a several malware techniques . Each technique has its own advantages and disadvantages. Mobile malware steals

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the information and affect the mobile phones in many ways. So prevention is required to mobile phones from the malwares. In order to overcome the signature based detection, to propose and implement a new approach is called n-gram analysis which is used to detect the new malwares in mobile applications.

REFERENCES

[1] Marwa M.A.Elfattah et al., "Handsets Malware Threats and Facing Techniques" , International Journal of Advanced Computer Science and Applications , Vol.2,No.12,pp 42-48,2011.
[2] A.Bose et al .,"On Mobile Viruses Exploiting Messaging and Bluetooth Services", IEEE International Conference on Security and Privacy in Communication Networks, Secure Communication, pp 1-10,2006.
[3] P.Vinod et al., "Survey on Malware Detection Methods,3rd Hackers " Workshop on Computer and Security, pp 74-79,2009.
[4] A.Bose et al., "Behavioral Detection of Malware on Mobile Handsets", IEEE International Conference on Mobile Systems, Applications, Services , pp 225-238,2008.
[5] Abou-Assaleh et al., "N-gram based detection of new malicious code" IEEE Annual International Conference on Computer Software Applications, Vol.2,pp41-42,2004.
[6] Igor Santos et al., "N-gram Based File Signatures for Malware Detection ", International Conference on Enterprise Information Systems(ICEIS), pp 317-320,2009.
[7] M.Schultz et al., "Data Mining Methods for Detection of New Malicious Executables" IEEE Symposium on Security and Privacy , pp 38-49, 2001.
[8] Kirti Mathur et al., "A Survey on Techniques in Detection analyzing malware executables" International Journal of Advanced Research in Computer Science and Software Engineering", Vol.3,Issues 4,pp 422-428,2013.