Techniques Used for Detection of Mobile Spyware

Neelam Kaur
Lovely Professional University, India

ABSTRACT : *Spyware is an unwanted software that steals bank account details and other confidential information and sends back to the attacker from where the spyware originated. The attacker makes use of this information to send spam messages according to the location of the user. They can also cause a financial loss to the user. The spyware attack on Smartphone has increased with the drastic increase in the number of Smartphone users. Smartphone is widely used all over the world for communication, banking transactions and for many other purposes. These phones have lots of functionality to support user's demand and this is one of the main reasons which make it difficult to detect the spyware. There are different types of techniques available to detect the spyware. The different techniques are signature based, behavioral based and data mining based. In this paper, pros and cons of each technique have been discussed.*

Keyword-*Smartphone, Spyware*.

1. Introduction

Smartphone is a phone which is not only used for calling but for many other purposes also. It helps in communication in the form of calls, messages, emails, and many other things. It is full of advanced features. These advanced features are so attractive that now majority of the population uses smart phone as compared to normal mobile phone. The increased demand has raised security and privacy issues for the user's smart phone. The attacker can gain the confidential data that the used has stored on the smart phone. The attacker can get location based information also by which user can be sent advertisements. The attacker if gains data related with bank account then that can be very harmful for the user and there may be a loss of money.

Smartphone is a phone which not only provides us the facility of calling but also other facilities like surfing, email, different types of messaging and many other facilities. User can download applications and the choice of applications is not limited. The number of people using Smartphone is increasing at a very fast pace. The portability and the features it supports have made its demand go higher.

Users now store all kind of data in their Smartphone as its portable and they can access their data by being at any place and whenever they want. Users use it for storing their personal data, credit card details and for many other purposes. There are different kinds of privacy and security threats to a Smartphone. Smartphone contains logs and logs contain information about all the activities user has done. Logs can be misused to send advertisements based on location. So in this paper the detection techniques of spyware is discussed so that the user comes to know if the spyware is infected by a spyware.[1][2]

2. Smartphone Threats and Attacks

Smart phones are under many threats and attacks. Few threats and attacks are summarized below:[3][4]

2.1 Spam

A spam can enter a smart phone through emails or Multimedia messages. Spam emails or messages may include links which direct users to phishing websites. Spam can also be used to cause denial of service attacks.

2.2 Phishing

It is a way to steal user name, password, credit card details, and other personal information by masquerading as a trusted identity. These attacks are present in social networking websites, emails, and Multimedia messages, etc and what they do is that they contain links and those links redirect the user to a website. If user fills in its username and password then attacker gets that information and can further use it.

2.3 Spoofing

An attacker can pretend to be some other identity or a trusted identity. Attacker sends the messages but it appears to have come from a trusted party or some other identity.

2.4 Sniffing

It is called as eaves dropping a smart phone. It was shown that GSM's encryption for call and SMS privacy could be broken in less than a minute. There are different ways to tap a smart phone.

2.5 Vishing

It involves voice and phishing. It is an attack in which the attacker tries to gain access to private and financial information from a smart phone user. An attacker calls the user and pretends to be a trusted party and the user provides their personal information.

2.6 Pharming

Attacker can redirect web traffic in a smart phone to a malicious website. Attacker collects smart phone's user information and after that few specific attacks are possible. For example, when a smart phone is used to browse a website, the HTTP header includes some information which can be used to start some other attacks on the smart phone.

2.7 Denial of Service attack

Text messages or incoming calls can be used by the attacker to commit this attack. Receiving hundreds of messages and calls could disable a smart phone.

3. Spyware

Spyware is a type of unwanted software which is very harmful for Smartphone users. Spyware comes under malware. Malware also includes virus and Trojan. An android smart phone user downloads many applications from the application store. Fig. 3.1 shows that the attacker selects an application, and then modifies that application to add malicious code and publish it on the application store. Any user, who downloads that particular application on their smart phone, will also get the spyware. Once this spyware is in the smart phone, it will start its job of stealing personal information of the user and will send the collected information to the attacker.

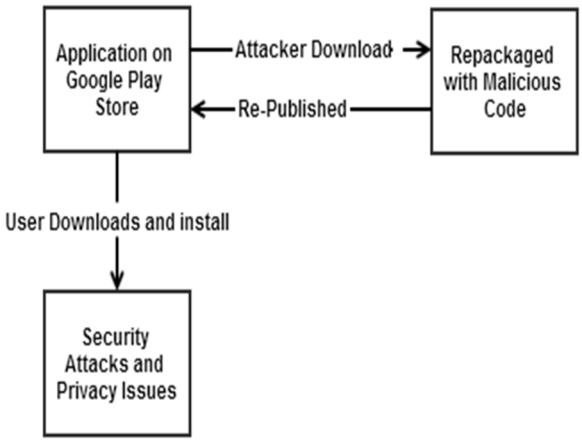

Figure 3.1 Malicious application enters into the Smartphone

Spyware can access logs as well. These logs can be used to know the location of the user and then user can be sent spam advertisements based on location and the user privacy is compromised. Sometimes more sensitive information is sent to the remote server like email account login details, phone number, IP address, etc. All these details compromise the privacy of user. There should be a control mechanism which the user can use to restrict usage information. Usage patterns should be protected from the third party. [5]

Researchers are trying to find ways in which these spywares can be detected and blocked to send out user's personal information. Detection and prevention of spywares requires antispyware and not a general anti-virus because these anti-viruses do not give much attention to spywares as they are multi-purpose.[5]

Smart phone user notices that the smart phone performance has decreased as it runs slow and most of the time it hangs. Spyware makes use of network to send data out to attacker so it does not let user internet. There should be some method to watch the activities of the android application and if they misbehave then immediately action should be taken.

4. Spyware Detection Techniques

4.1 Signature Based Detection

In signature based detection, the signature database is manually constructed by expects who have relevant knowledge and experience. Signature based anti-spywares use the database for matching with the signatures of the applications. Signature based detection is just a pattern matching technique, so it's very simple to implement and it takes less time for detection as compared to other detection techniques.

There are few problems with signature based detection. Firstly the signature database is created manually so it may involve human error. Secondly they cannot detect attacks which involve simple transformation and they can be easily evaded. Thirdly the database needs to be updated regularly so that the false negative rate does not increase.[6]

4.2 Behavior Based Detection

Signature of known spyware is matched against applications which are installed. By doing some obfuscation transformation, signature based technique can be easily evaded. [7][8]

Spyware's behavior is difficult to define as there are so many ways in which they behave and the level of harm they cause also vary. Researcher proposed behavior based detection for accurate detection of spyware. Behavior based detection do not depend on binary representation of the spyware so its better as compared with signature based detection technique as they can detect entire classes of spyware and even

obfuscation cannot help the spyware creator to cross the anti-spyware using behavior based detection technique.

Behavior based anti-spyware have a database which contains the malicious and non-malicious applications behavior which is used to detect the spyware. Behavior based anti-spyware mainly focus on web-based interfaces as through this spyware can collect confidential data and can monitor user activities. Use of behavior based detection helps us detect the unseen spyware as it checks the application behavior.

There are few problems with behavior based detection. Firstly it is difficult to construct the behavior based database as it involves lots of complexities. Secondly the database needs to be updated from time to time to keep the false positive rate and false negative rate low.

4.3 Data Mining Based Detection

In Data Mining Based Detection of spyware, a classifier is used to classify the application as a spyware or not. The classifier is made from the training set generated using the malicious and non-malicious databases. When the classifier is built the different attributes are chosen on the basis of one of the attribute selection methods. The purpose of this selection method is to make the classification process of the application very fast. The classifier is made using data mining algorithm. The algorithm should be chosen carefully as the accuracy of the anti-spyware depends on it. The test set is used to test the classification accuracy of the classifier. All the tuples in the test set are classified by the classifier. The number of tuples correctly classified helps in calculating the accuracy of the anti-spyware. [9]

Data mining based anti-spyware can detect known as well as new spywares and it do not use signature matching so it cannot be evaded by using simple transformations. The accuracy of this technique is much more than that of signature based detection.

5. Conclusion

The techniques discussed are the major techniques used by the anti-spyware tools for detection. Data mining based detection technique is the one which provides greater accuracy as compared to the others. The accuracy of the detection can be further improved by combining different techniques that means it will further decrease the false positive and false negative rate. The techniques used for the detection should be combined or a new detection technique should be constructed by keeping in mind the resource constraints of the Smart phones.

References

[1] R. Shams, M. Farhan, S. khan, F. Hashmi, Comparing Anti Spyware Products – A different Approach, *IEEE*, 2011, 75-80.

[2] T. Weil, A. Jengi, H. Lee, C. Chen, C. Tien, Android Privacy, *International Conference on Machine Learning and Cybernetics*, 2012, 1830-1837.

[3] J. Mu, A. Cui1, J. Rao, Android Mobile Security – Threats and Protection,*International Conference on Computer, Networks and Communication Engineering*, 2013, 683-686.

[4] H. Rui, J. Gang, W. Liang , Security Mechanism Analysis of Open-Source Andriod OS & Symbian OS, IEEE, 2012, 3497-3501.

[5] S. Datta, C. Bonnet, N. Nikaein, Android Power Management: Current and Future Trends, *IEEE*, 2012, 48-53.

[6] D. Venugopal, G. Hu, Efficient signature based malware detection on mobile devices, *Mobile Information Systems, 4(1)*, 2008, 33-40.

[7] A. Shabtai, U. Kanonov, Y. Elovici , C. Glezer, Y. Weiss, Andromaly: a behavioral malware detection framework for android devices, *Springer*, 2012, 161–190.

[8] A. Bose, X. Kang, G. Shin, T. Park, Behavioral Detection of Malware on Mobile Handsets, *ACM*, 2008, 225-238.

[9] S. Shirbhate, Dr V. Thakare, Dr S. Sherekar, Data Mining Approaches For Network Intrusion Detection System, *International Journal of Computer Technology and Electronics Engineering (IJCTEE) National Conference on Emerging Trends in Computer Science and Information Technology*, 2011, 41-44.