International Journal of Computer & Mathematical Sciences
IJCMS
ISSN 2347 – 8527
Volume 6, Issue 9
September 2017

A Survey: Trojan horse Detection Techniques in Network

Falgunikumari Chaudhari[#1], Shehnaz Patel[*2]

[#1]PG Scholar, Department of Information Technology, SVM institute of Technology, Bharuch , India.

*2 Assistant Professor, Department of Information Technology, SVM institute of Technology, Bharuch , India

Abstract-In Present time lots of data are transmitted over the network as download and upload. During downloading and uploading process various types of attacks may be possible. Likewise malware, Trojan horse or many warms. This paper proposes a Trojan horse detection techniques during data upload and download. There are many methods for Trojan horse detection, viz., machine learning method, weighted voting method, keep alive method, master slave connection method etc. The paper also detects keep-alive behaviour in a flow and gets correct judgment and make White list and Black list.

Keywords–*Trojan horse, Keep-alive, Machine-learning, Weighted-voting*

I. INTRODUCTION

Trojan horse is one type of malware which makes some unwanted changes in system [1]. Trojan horse is not exactly virus but sometimes it behaves like virus [2]. There are various types of Trojan horse likes: Remote access Trojan, Data sending Trojan, Destructive Trojan, Security software disables Trojan, Denial of service attack Trojan. Remote access Trojan horse completely accesses the user's system. This type of Trojan horse hides in small size applications and games of user's system [2]. Data sending Trojan horse provide the sensitive data like password, debit card details, log files or email's details to attackers [2]. Destructive Trojan horse deletes important files of user's and this type Trojan horse can't be detected easily [2]. Security software disables Trojan is one type of antivirus which is use as firewall without knowing user and it is mostly combined with payload [2]. Denials of service attack Trojan makes flooding on network and creates more traffic on network [2]. The Trojan horse inserts in the system via transmission of configuration bit stream over the network, compromise the security of computer system application [3]. Nowadays attacks are in form of combination of Trojan horse and spyware in various operating systems [4]. It theft user's information likes login information, username and password, personal files, Images or chat logs[4].Trojan horse are similar to other computer programs but it makes some unauthorized actions in computer[5]. Trojan horse gives remote access of computer to the hacker [5]. Trojan horse can't run without the use's initial permission [5]. The word Trojan horse derived from the story of big handmade horse used to trick defender of troy in war [6]. Trojan horse is able to leak sensitive data from the system [6]. The backdoor Trojan horse bypasses security mechanisms and accesses the system [6].When Trojan horse attacks on two way protocol is very complex and it challenges for security [7].If Trojan horse is in chip that was very danger for system and network [8]. Here the Trojan horse is difficult to detect because the Trojan horse is inserted only at the time of manufacturing [8]. If the Trojan horse is there in the network, it destroys the three major security concern likes: leaking confidential information, Secrete key and changing or disabling the original data [9]. When Data is uploaded in the network or downloaded from the network, the Trojan makes changes in the data and corrupt the data[10]. When Trojan horse receive small size packet, it increases the packet size and send big size packet on network and increases the work load of network [10].

II. METHODS TO DETECT TROJAN HORSE IN NETWORK

A. In paper [3] authors describe the method for Trojan horse detection using file programmable gate array(FPGA) with Dynamic reconfiguration of circuit implemented on network. It theft the data from system and transmit data over the network. Trojan horse insertion is done via transmission of configuration bit streams over the network to compromise the security of one or more applications. Following are the various types of attacks on crypto graphics core:

a. Attack on AES encryption circuit

b. Attack on TRNG

c. Attack on processor based AES encryption

d. Attack on processor based cash machine algorithms

Here the leakage of cryptographic keys is demonstrated, biasing the probability of 0s and 1s in the output bit stream, and threats to processor implementations of secure applications.

B. Five techniques for detection of Trojan horse is described in [4]:

a. Spyware Detection Techniques

b. Signature Based Detection

c. Behaviour Based Detection

d. Data Mining Based Detection

e. Advanced Behaviour Detection

Spyware detection and signature based detection are detecting the Trojan horse in device which is transmitting data over the network. Behaviour based detection, data mining based detection and advance behaviour detection techniques detects weather the Trojan horse malware exist or not and remove the Trojan horse. Here these all techniques detect only the Trojan horse already exist in the system. It can't prevent the Trojan horse from the network.

C. In paper [5] the authors have described the two methods for Trojan horse detection,

a. Windows Dynamic Link Library

b. Machine learning Method

Both methods collect some sample of data and store it in database and make analysis. After that it checks whether the Trojan horse is in the system or not. In these methods signature based technology is used.

Window Dynamic link library method creates a new signature based on old signature.

The machine-learning method comprises of the instance-based learner, decision tree and feature selection. This involves collecting a few samples of the data and storing them in a database and then analysing them through these machine-learning methods.

D. The authors in [6] described two methods for detection of Trojan horse:

a. Destructive method

b. Non Destructive method

Destructive method is easiest method to detect the Trojan horse to protective layer and open and check by reverse engineering techniques, but sometimes this method destroy the System structure.

Non Destructive method is costly then destructive method but it can't destroy the system structure. In this method data are saved in database and make analysis for detection of Trojan horse.

E. In paper [7] the authors have described two attacks of Trojan horse:

a. Delay photon attack and

b. Invisible photon attack.

These attacks are on protocol of network. Sometimes these attacks are on two way protocol and removal of the Trojan horse is very difficult. At that situation Quantum key distribution (QKD) technique is used to prevent the attack.

In Quantum key distribution (QKD) method, it measure the delay time of sending or receiving data from the network and detect the Trojan horse. The drawback of QKD method is the protocol is not properly modified and sometimes it can't work properly.

F. The authors in [8] described two detection techniques:

a. Simple voting

b. Weighted voting

Simple voting method detects the Trojan horse by analysis of side channels. It measures bit level democratic majority and make output.

Weighted voting method is same as simple voting but it measures multiple side channels at same time. Weighted Voting method is only useful during data uploading or downloading.

G. In paper [9] the authors said that sometimes the Trojan horse attack may be inside or outside due to denial of service. Here Trojan horse detection is done using the side channel information. The side channels obtain the power signature. These methods apply input check to detect if the Trojan horse is present or not and also measure the power consumption. If the Trojan horse is detected then reverse engineering is applied.

H. The authors in[10]said that Trojan horse receive small packets and make large packet by multiplying packets and transmit data to the network. Here there are two techniques for Trojan horse detection:

a. Keep-alive

b .Master slave connection

Keep-alive method uses machine learning method to detect Trojan horse. It finds high frequency coefficient with keep-alive behaviour. Keep Live Method is fast match method and scan all the

packets.94% Trojan horse are detected using Keep alive method.

Master Slave connection method generates the signature code and matches the data over the network. It collects API call sequence and generates vector and match the packet.

III. CONCLUSION

Here Various Techniques for Trojan horse detection likes Spyware Detection Techniques, Signature Based Detection, Machine learning Method, Destructive method, Non Destructive method, weighted voting, keep-alive and Master slave etc. are described. Among all these methods Keep Alive method is faster than any other method. This method is efficient and provides good-performance. Keep-alive method detects the Trojan horse as per network behaviour. This method also describes the black list and white list as per the effect of Trojan horse on the system in network. Nowadays the data leakage is a big problem and mostly the Keep Live method is used to detect the Trojan horse and prevent data leakage.

If the keep-alive and API call methods can be combined than it can make more accurate result on network behaviour. We can make the proper black list or white list of Trojan horse attacks based on keep-alive method.

REFERENCES

[1] seminartopics.in, 'computer seminar topics', 2017. [Online].Available:http://www.seminartopics.in/computer%20seminar%20topics/Trojan-Horse.php. [Accessed: 23- July- 2017].

[2] webopedia.com, 'what is Trojan horse', 2017. [Online]. Available: http://www.webopedia.com/TERM/T/Trojan_horse.html [Accessed: 27- July- 2017].

[3] Johnson, Anju P., et al. "Remote Dynamic Partial Reconfiguration: A Threat to Internet-of-Things and Embedded Security Applications." *Microprocessors and Microsystems* (2017).

[4] Abualola, Huda, et al. "An Android-based Trojan Spyware to Study the Notification Listener Service Vulnerability." *Procedia Computer Science* 83 (2016): 465-471.

[5] Gudipati, Vamshi Krishna, et al. "Detection of Trojan Horses by the analysis of system behavior and data packets." *Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island*. IEEE, 2015.

[6] Ehsan, Sharifi, et al. "Performance analysis of Hardware Trojan detection methods." *International Journal of Open Information Technologies* 3.5 (2015).

[7] Yang, Xiuqing, et al. "Trojan horse attacks on counterfactual quantum key distribution." *Physics Letters A* 380.18 (2016): 1589-1592.

[8] Amin, Hany AM, Yousra Alkabani, and Gamal MI Selim. "System-level protection and hardware Trojan detection using weighted voting." *Journal of advanced research* 5.4 (2014): 499-505.

[9] Aliyu, Ahmed, et al. "Hardware Trojan Model For Attack And Detection Techniques."*International journal of Scientific and Technology research* (2014):102-105.

[10] Pu, Yiguo, et al. "Data stolen Trojan detection based on network behaviours." *Procedia Computer Science* 17 (2013): 828-835.