2012 International Conference on Image, Vision and Computing (ICIVC 2012)
IPCSIT vol. 50 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V50.32

Research on the Model of Distributed Trojan Horses Cooperative Concealment

LIU Lan [+] and YUAN Dao-hua

School of Computer Sicence, Sichuan University, ChengDu, Sichuan, 610065, China

Abstract. The concealing technology of Trojan horses which determines the concealing capability and the life cycle of Trojan is one of the most important technologies in Trojan horse. This paper puts forward a model of distributed Trojan Horses cooperative concealment. This model can reflect the variation rate of Trojan horses and the migration status of hosts and so on. Experiment results demonstrate that it can improve the concealment capability of Trojan and reduce the probability of remote control being found.

Keywords: Trojan Horse, Concealing Technology of Trojan, Trojans Cooperative Concealment, Distributed Cooperative Concealment of Trojan horse, Model of Distributed Trojans Cooperative Concealment

1. Introduction

Trojan horse is a kind of vicious procedure [1] which can hide in computer secretly and remote other's computer illegally. It can be used to steal other's information by network attacker. The whole nation analysis report of state and investigation of computer virus epidemic situation show that the activity of using virus and Trojan horse for illegal property is on the rise.

Trojan horse has strong concealment so that it can hide in computer for a long time. It is difficult for non-professionals to find it. Trojan concealment technology can be approximately divided into file concealment, process concealment, communication concealment and cooperation concealment and so on. The first three Trojan concealment technologies mainly use single host as their concealment carrier. However, Cooperate concealment mainly uses multiple hosts as its concealment carrier to realize multiple hosts' cooperative concealment.

This paper introduces a model of Trojans cooperative concealment, and analyzes some related parameters in the model. The experiment shows that it can implement the ability of Trojan cooperative concealment well.

2. Related Work

Fred Cohen et al [2,3] have an in-depth study of computer viruses. They take Trojans as a special case of computer viruses, and give a mathematical model of Trojan horses and viruses. Thimbleby et al [4] studied the model of viruses, and gave a formal model of Trojan. At the same time, they described the hidden characters of Trojan, but they did not research the cooperative concealment of Trojans. According to the feature of Trojan, Qiao Jun-Jian et al [5] gave a propagation model of Trojan and virus. But they did not research the Trojans concealment ability in their paper. Zhang Xin-Yu et al [6] studied the Linux Trojan hiding technology and proposed an idea of Trojans cooperative concealment. But they didn't research the

[+] Corresponding author. Tel.: + (18782262186).
E-mail address: (shuimenjian@126.com).

model of Trojan cooperative concealment. Kang Zhi-ping et al [7] proposed a Trojan structure named "many-to-many", which can implement the Trojan cooperate concealment, but it can't analyze the model of Trojan cooperative concealment. Hu Bo et al [8] add some intelligence to Trojans, and proposed a Trojan model of function atomization and system intellectualization. But it also did not research the Trojan's cooperative concealment in the paper.

For the above case study, we did a co-depth analysis on the model of a Trojans cooperative concealment, and proposed a model of distributed Trojan cooperate concealment.

3. Idea of Trojan Cooperative Concealment

Trojan cooperate concealment technology casts off the lack of traditional Trojan concealment which is only applied to single Trojan. It improves the whole concealment of Trojan through the cooperation among Trojans.

Zhang Xin-yu, who refered to the Trojan model proposed by Thimbleby[4], gave the formal description of Trojans cooperate concealment[6], as follows:

Take as a primary Trojan, as sub Trojans. Every can perform attribute of concealment of whole Trojan. They can hide the characteristics of together.

$$\text{Suppose}: r, r', \hat{r}, \hat{r}', ri, \hat{r}i, ri', \hat{r}'i \in R,\quad \hat{u}i, i \in [1, k],\quad k \geq n$$

$$\wedge ri \sim \hat{r}i$$

$$\wedge E(ri)\hat{u}i \approx E(\hat{r}i)\hat{u}i$$

$$\wedge M \quad t \in L^*$$

$$\wedge [\![E(ri)\hat{u}i]\!] ri \xrightarrow{t} r'i$$

$$\wedge [\![E(ri)\hat{u}i]\!] \hat{r}i \xrightarrow{t} \hat{r}i'$$

$$\wedge ri' \neq \hat{r}i'$$

$$\wedge r \sim \hat{r}$$

$$\wedge \hat{u}i \in L^*$$

$$\wedge [\![E(r)\hat{p}]\!] r \xrightarrow{\hat{u}i} r'$$

$$\wedge [\![E(\hat{r})\hat{p}]\!] \hat{r} \xrightarrow{\hat{u}i} \hat{r}'$$

$$\begin{cases} \wedge r' \neq \hat{r}' & 1 \leq i \leq n \\ \wedge r' \sim \hat{r}' & i \geq n \end{cases} \qquad \hat{u}i \text{ help } \hat{p} \textit{ for hiding}$$

From the above described [4,6], we know that can change the state of system. Sub Trojans can help to implement attribute concealment. Testing procedures can not distinguish between and normal for most parameters through cooperate work among multiple sub Trojans. Formal description of Trojan cooperate concealment show that assist in achieving the introduction of sub Trojans can improve the hidden capability of whole Trojan.

4. Distributed Trojans Cooperate Concealment Model

4.1. Outline of the model

This model takes the whole network as Trojan horse hiding carrier. When the Trojan is implanted in a host, it uses its own vulnerability scanning detection function to detect the rest hosts of the network. After the host with vulnerability is detected, Trojan is implanted itself into the host using vulnerability loophole. Based on this, Trojan program's self-spreading is realized successfully. Trojans use this way of spreading to control the rest hosts gradually. Trojan which first spread into network is called primary or agent Trojan which is the core of model and responsible for accepting and executing remote instructions of controlling terminal as well as monitoring the rest Trojans of the same network. Excluded the primary Trojan horse, the

rest Trojans of the network is called sub-Trojans or common Trojans which form the concrete elements of model, and they account for accepting and executing instructions from primary Trojan.

4.2. Analyzes the model

There are three forms of hosts in the model: Trojan hosts, susceptible hosts and immune hosts. As follows:

1) Trojan host (T): this host has been infected with Trojans (primary or sub Trojan horse).

2) Susceptible host (S): this host is not infected with Trojans, but it may be detected and injected Trojans by the primary Trojan horse.

3) Immune host (I): this host is installed of specific patches against these Trojans, and after the Trojans are removed, it won't be infected by this kind of Trojan.

To simplify the model, we make some following assumptions:

1) The size of network is unchanged which means that the number of network hosts N(t) is unchanged.

2) The host's state of the migrated is completed within a time unit; this means that Trojan is injected into the host also within a time unit.

There are some required parameters should be defined first. As follows:

$N(t)$: Total Number of hosts in the network.

$T(t)$: Number of infected hosts in the network.

$S(t)$: Number of susceptible hosts in the network.

$I(t)$: Number of immunized hosts in the network.

$D(t)$: Number of rest hosts detected by primary Trojan.

P_k : Probability of Trojan being killed.

P_i: Probability of susceptible host infected Trojan.

P_f: Probability of Trojan being found.

The hosts only be in the status of susceptible or controlled by Trojans When ignorance of the status of immune. So, we should analyze the susceptible status and Trojan status in depth.

4.2.1. Changing rate of Trojan hosts

- Hosts from susceptible status changed into Trojan status

Primary Trojan can scan the rest hosts by IP address. In a unit time t, the number of susceptible hosts to be scanned is $D(t)$. So, the number of susceptible hosts changed into Trojan hosts is $D(t)PiPf$.

- Hosts from Trojan status changed into susceptible status

Within a unit time t, the probability of Trojan being found is P_f, the number of Trojans being found is $T(t)P_f$, so the number of Trojans to be cleared is $T(t)PfPk$.

Based on the above analysis, the equation of changing rate of Trojan hosts is:

$$dT(t)/d(t) = D(t)Pi - T(t)PfPk$$

4.2.2. Changing rate of Trojans

When one host is only infected by one Trojan, the number of Trojans is equal to the number of infected hosts in network, so the equation of changing rate of Trojan's number is also as follows:

$$dT(t)/d(t) = D(t)Pi - T(t)PfPk$$

4.2.3. Changing rate of susceptible hosts

Susceptible hosts changing rate is equal to the opposition of Trojan hosts changing rate. So the equation of the changing rate of susceptible hosts is:

$$dS(t)/d(t) = T(t)PfPk - D(t)Pi$$

So, following relationship exist in the model:

$$dT(t)/d(t) = D(t)Pi - T(t)PfPk$$

$$dS(t)/d(t) = T(t)PfPk - D(t)Pi$$

$$N(t) = T(t) + S(t)$$

4.2.4. Trojan hidden ability

This model can be seen as Trojan which hidden itself to other hosts in the network. So the hidden vector from a single host is extended to the entire network, thereby it increases the hidden ability and the life cycle.

When Trojan is hidden in the model, only all Trojans are exposed, the whole Trojan will be lost, so the concealment ability of model is associated with all Trojans. It can be expressed as H , the value of H is associated with $T(t)$, P_k P_i and so on.

5. Simulation Experiment

5.1. Experiment Introduction

We developed a remote control program as a Trojan in the experiment. The program can spread itself by using the system's loopholes. We select about 150 hosts, and 120 of them contain weak passwords loopholes. The following results are average experiments data, but it can basically represent the related features of Trojans, such as the rate of number changes of Trojans and the hidden property of control terminal. In view of the limited space of this article, we just give partial experiments results.

5.2. Experiment Result Analysis

Figure 1 examines the influence of initial value brings to the Trojans' number. The experiment result indicates that initial value can't influence the maximum number of Trojans. It only can influence the transition time of Trojans from maximum number to stable status.

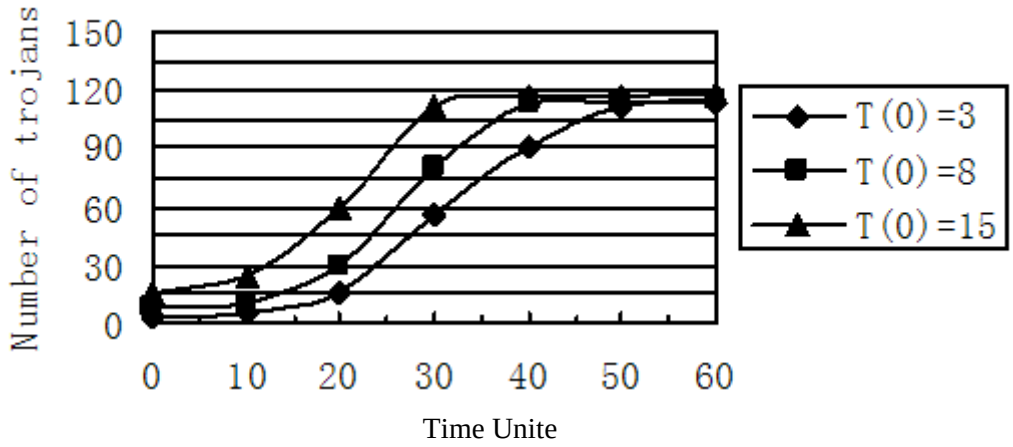

Fig. 1: Changing rate of Trojans effected by initial value of Trojans

Figure 2 examines the influence of host's anti-virus ability brings to the rate of Trojans. In the experiments, we respectively select partial hosts to install different security tools, and together with different virus libraries with different updated status. The experiment's result shows that the host's anti-virus ability can affect the maximum number of Trojans obviously.

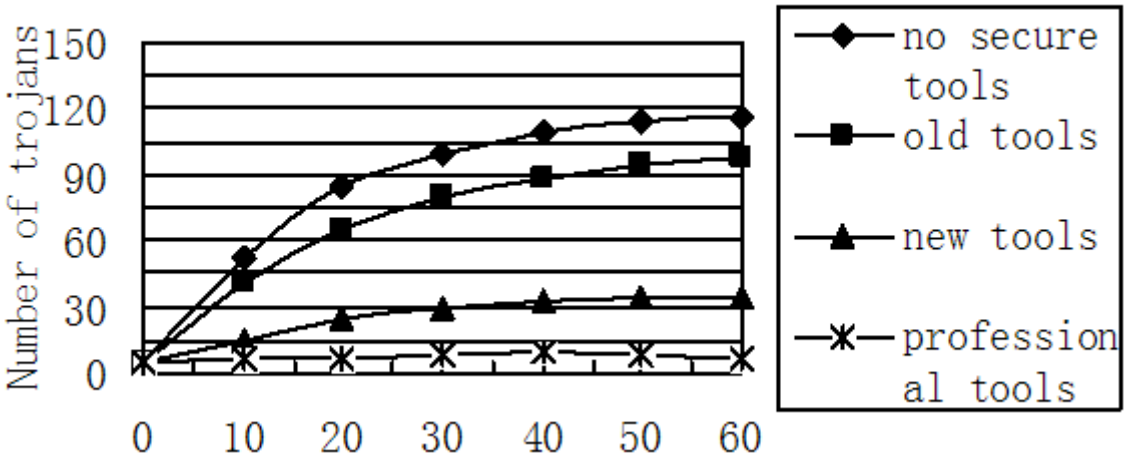

Fig. 2: Changing rate of Trojans effected by secure tools

Figure 3 examines how the number of the Trojans influences the hidden property of remote control terminal. The experiment result shows that the more the number of Trojans is, the harder the primary Trojan can be found. But, when the number of Trojans reaches a certain value, the possibility of sub Trojans can be found is increasing.

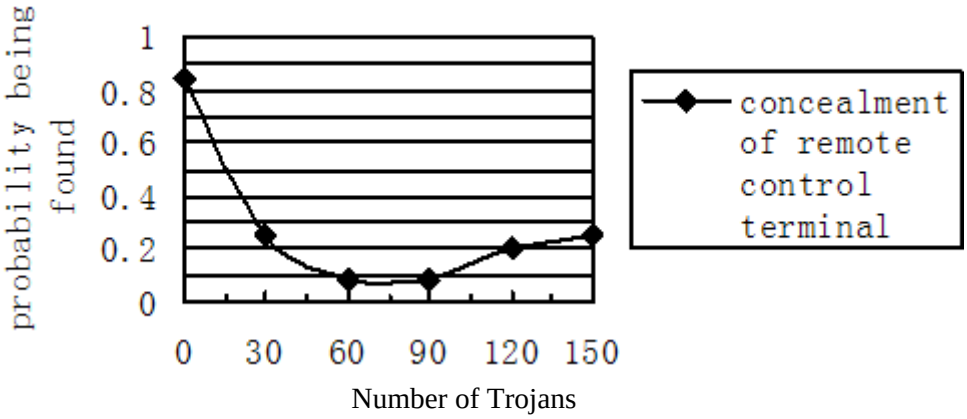

Fig. 3: Remote control terminal effected by the number of trojans

6. Summary and Prospect

According to the formal description of hidden thoughts of Trojans collaboration, this paper proposes a model of Trojans cooperative concealment. We analyze the parameters which are involved in the model. The experiment results show that this model can improve the overall hidden ability of Trojans, and decrease the possibility of which remote control terminal is found. However, the conclusion is only applied to small scale internal network. The next research is introducing this model to a large scale internet network, and studying its related features through more realistic network environment.

7. Acknowledgements

Thanks for my tutor and classmates and other person in my laboratory. They give me so much information and guidance for helping me to complete experiment and paper. Thanks for them.

8. References

[1] Baidu.Baike. malicious software. http://baike.baidu.com/view/362867.htm. 2010

[2] Adleman L M. “An abstract theory of computer viruses”.In:8th Annual International Cryptology Conference,Santa Barbara,California,USA,1988.

[3] Cohen F. “On the implications of computer viruses and methods of defense”. Computers and Security,1988,7(.2) ,pp. 167–184.

[4] Thimbleby H,Anderson S,Cairns P. “A framework for modelling Trojans and computer virus infection”. The Computer Journal,1998,41(7), pp. 444–458.

[5] Qiao Jun-Jian,Chen Ya-Ting,Li Xue-Fei. “Research of The Virus Trojan Transmisson Model”. Mathematics in Practice and Theory,2010,40(12) ,pp. 144–147.

[6] Zhang Xin-yu,Qin Si-han and Ma Heng-tai, et al. “Research on the concealing technology of Trojan horses”. Journal of China Institute of Communications,2004,25(7) ,pp. 153–157.

[7] Kang Zhi-ping,Xiang Hong. “Research and Practice on the Concealing Technology of Trojan Horses”. Computer Engineering and Applications,2006,42(09) ,pp. 103–105.

[8] Hu Bo,Cao Jiu-Xin,Sun Xue-Sheng,Yao Yi,Liu Yong-Sheng. “Research on self-adaptive Trojan horse model based on function atomization”.2010,31(12), pp.2683–2694.