Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 50 (2012) 10363-10365

ISSN: 2229-712X

Detection of m-worm to provide secure computing in social networks

M. Milton Joe[1], R.S. Shaji[2], F.Ramesh Dhanaseelan[1]

[1]Department of Computer Applications, St.Xavier's Catholic College of Engineering, Nagercoil-629 003.

[2]Department of IT Noorul Islam University Thakulay.

ARTICLE INFO

Article history:

Received: 14 June 2012;

Received in revised form:

16 August 2012;

Accepted: 8 September 2012;

Keywords

M-worm,

Social network,

Secure computing.

ABSTRACT

Worms can be classified into various categories; one among them is active worms. These active worms pose a vital security threats to the internet especially in social networks. Defending against such active worms are not as easy as other types of worms. Active worms propagate in an automatic fashion such that it can infect as many as clients. In this paper we evaluate a special type of active worm, called muffle worm (M-worm in short). The m-worm is different from any other worms, for it goes undetected when the scan process encountered. The m-worm identifies the vulnerable clients in the social networks and infects the client. Once the client is infected, then the infected host scans for the other vulnerable clients and infects the client. We studied the comprehensive characteristics of the m-worm and provide the secure computing in the social networks. The scheme that we propose detects the m-worm from where it has been propagated and the current location of the worm. Once the origin of the m-worm is identified, the client that spread the m-worm can be disconnected from the social networks (Blocking). Thus the secure computing can be obviously provided in the networks. Still if the misbehaved client wishes to participate in the communicating network, which would be done by authenticating the corresponding client. The proposed scheme proves that it could provide secure computing in the social networks.

Introduction

Worm refers to a software program that acts in an abnormal way in the computing system and destroys the normal process of any computing system. These worms are mainly divided into two categories: 1) Structured worm, 2) Unstructured worm. The first type of worm needs an existing program to pass on from one host to another host (using the pen drive to copy the file from one system to another system).

The second type of worm gives the challenge to the programmers to defend against them, for it does not need an existing program to propagate from one host to another host(like structured worm). These worms identify the vulnerable host in the network(less or no security) and automatically propagate to the less security host.

This type of unstructured worm is known as active worm, because of its automatic propagating nature. Identifying and defending such active worms are not an easy task. In this paper we evaluate a special type of active worm referred as m-worm.

Active worms

Active worms are similar to any other virus, for its self propagating nature. As we all know that social networks refer that at a time more than one client participates in the communication. These active worm scans for the vulnerable host in the social networks and automatically propagates to the host to infect it. Once the host is infected, further the infected host scans for the other vulnerable host in the social networks and infect them.

This process continues until all the less security hosts are infected in the social networks or the networking is disconnected. Once the m-worm infects the host, then it cannot communicate in the social network in the proper way and it will also infect the other host in the network.

Detection of any worm

Worm refers to a software program that makes the computing system to work in an abnormal way. Usually worm can be identified in any system by going for scan strategies. When the scan process is encountered, it identifies the various types of worms that are resided inside the system. It is normally being done by anti-software programs. Once the worm has been found in the host, that can be deleted to provide wormless operation in the host.

It is quite different from the above worm that goes undetected when the scan process in encountered. Such worms are known as active worms. Here in this paper, we refer a special type of worm known as m-worm, which always goes undetected when scan process occurs. Defending against the m-worm is a very difficult task. A new mechanism should be provided to encounter the m-worm that propagates in the social networks.

M-worm propagation

A special type of active worm that we refer in this paper is m-worm. This m-worm has the nature of propagating form one host to another host in an automatic fashion. In every social networks, there should be more than one host participate in the communication. This m-worm searches for the host in the networks and identifies the host that is vulnerable. Once the vulnerable host is identified the m-worm moves to that particular host and infects it as shown in the figure 1.

This automatic propagation of m-worm cannot be stopped until all the hosts are securable. This propagation of m-worm must be stopped in the earlier stage itself to provide the secure computing in the social networks. Here, we prove that the m-worm propagation can be identified in the social networks and that could be stopped in the beginning itself.

Tele:

E-mail addresses: m.miltonjoe@gmail.com

Fig 1 Worm Propagation

System Architecture

As shown in the figure 2, the worm identifies the vulnerable host and infects it. The infected host could scan for the worm and notified from which host the worm spread. Once the worm spread host is identified the host can block the worm spread host from the social networks as shown. The blocked host can be admitted in the network after authenticating, if it wishes to communicate with host as shown in the figure 2.

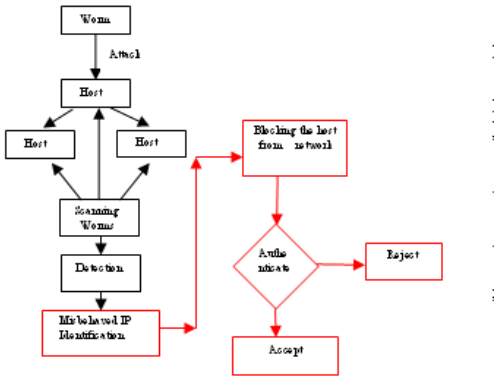

Fig 2 Architecture

Algorithm

```
m= worm;
scan hosts in the network;
While (host ==vulnerable)
{
host= m;
infected host scans in the network;
if (host 1== vulnerable)
{
host 1=m;
}
}
Infected host scans for detection;
If(m found)
{
wsh=detect worm spread host;
loc=detect the worm and its location;
}
else
{
no worm;
valid data;
}
If(wsh==true)
{
block wsh from the network;
}
while(blocked wsh sends data)
{
validate the data;
If(no worm)
{
accept the blocked wsh;
}
else
{
reject the blocked wsh;
}
}
```

Detection of m-worm

Defending against this type of m-worm is not as easy as we think of any other worm. The detection of m-worm can be carried out in major two ways: 1) Host based detection; 2) Network based detection. The first way of detection can be carried out by monitoring each host in every periodically time. The second way of detection can be carried out through the monitoring the entire network in every period of time.

Here, we could make use of network based detection scheme to detect the m-worm in the social networks. The m-worm can be detected by monitoring the social network in every period of time. The data can be passed among hosts as packets. These packets can be monitored and routed to the destination through routers and monitoring centers.

Sometimes the m-worm goes undetected during the scan process. We prove that the m-worm can be detected by the threshold value that is applied in the detection scheme to differentiate the normal packets from the worm packet. Thus m-worm can be detected and secure computing can be provided in the social networks as shown in the figure 3.

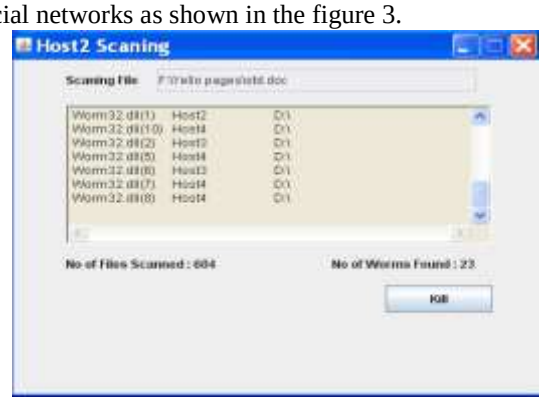

Fig 3 Worm Detection

Performance evaluation

The performance of our m-worm detection could be evaluated by the following metrics: 1) Infection Ratio (IR) which defines the number of computers infected in the total number of vulnerable computers. 2) Detection Rate (DR) which defines the time taken to detect the worm propagation from the time of worm started to propagate.3) Blocking Host (BH) which defines the host that spread the worm in the network can be blocked from the communication and further if the blocked host wishes to participate in the communicating network that could be done to authenticating the host. Our evaluation schemes proves that these metrics could be achieved in an efficient manner

Experimental Results

Blocking the host

As shown in the fig 4 the misbehaved host can be blocked from the communicating network. When the infected host scans for the worm, it will be notified from which host the worm spread. Once the worm spread host is identified the victim host can block the misbehaved the host as shown below.

Fig 4 Blocking the Host

Authenticating the host

If the blocked the host wants to participate in the communicating network that can be done through authenticating the host as shown below in the fig 5. When the blocked host sends packet(data) to the host, the host will be notified that the misbehaved host wants to communicate. Once the notification arrived the destination, the host can simply either deny the communication with the host or it can scan the packet whether it contains worm or not. If the packet has worm it can be rejected otherwise the misbahaved host would be allowed in the communicating network.

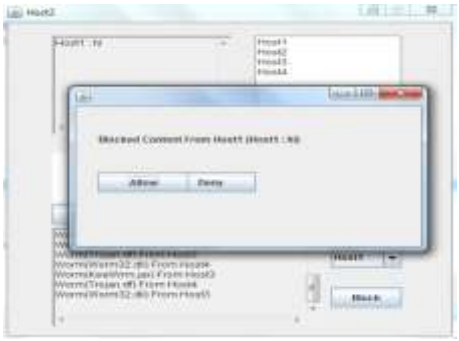

Fig 5 Authenticating the host

Conclusion

In this paper, we studied a special type of active worm referred as m-worm, which propagates in an automatic fashion. This m-worm goes undetected, when scan process encountered. Our m-worm detection process successfully detects the m-worm propagation along with above mentioned metrics. Our future study would be other smart worms and its characteristics.

References

[1] Wei Yu, Xun Wang, Prasad Calyam, Dong Xuan and Wei Zhao, “Modeling and Detection of Camouflaging Worm”, IEEE Transactions on Dependable and Secure Computing, Vol.8, No.3, May-June 2011.

[2] D. Moore, V. Paxson, and S. Savage, “Inside the slammer worm,” in IEEE Magazine of Security and Privacy, July 2003.

[3] Z. S. Chen, L.X. Gao, and K. Kwiat, “Modeling the spread of active worms,” in Proceedings of the IEEE Conference on Computer Communications (INFOCOM), San Francisco, CA, March 2003.

[4] X. Wang, W. Yu, A. Champion, X. Fu, and D. Xuan, “Detecting worms via mining dynamic program execution,” in Proceedings of IEEE International Conference on Security and Privacy in Communication Networks (SECURECOMM), Nice, France, September 2007.

[5] C. C. Zou, D. Towsley, and W. Gong, “Modeling and simulation study of the propagation and defense of internet e-mail worm,” IEEE Transactions on Dependable and Secure Computing, vol. 4, no. 2, pp. 105–118, 2007.