IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Review- Computer Viruses In Networks

Ankur Singh Bist
Govind Ballabh Pant University of Agriculture And Technology, Panthnagar, India
ankur1990bist@gmail.com

Abstract

Computer viruses are serious threat for society . Computer virus get spread in wired and wireless networks and create various types of threats . For Tackling the problem of malicious activities , it is required to study the propagation modes of viruses in network so that this analysis may lead to design the defensive tool against these attacks.

Keywords: Intrusion , Network .

Introduction

The use of internet has become a common activity now a days and in parallel it caused the increment in the activities produced by computer viruses . The damaging activities caused by malicious codes are increasing day by day causing harm to society . There are various schemes that are designed to defend against computer viruses . Here we are focussing mainly on computer viruses study in networks . A lot of work has been done in the area of designing intrusion detection system in wireless sensor network but still the factors of efficiency of these proposed models needs improvement for better security schemes . Various study using simulation methods has been done to analyse the behaviour of computer viruses in network so that this problem can be recovered easily.

Detection Schemes

In a network setup virus get spread from any random end user and get spread in other cluster utilizing the hub . The diagram given below shows the different states of end user . Susceptible user remains under the fear of infection , when the infection occurs to end user it moves to infected state and on getting virus signatures the movement takes place in term of states from susceptible to immune and from infected to immune .

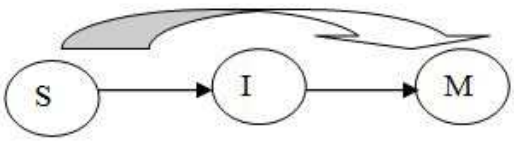

Fig1. Different States Of end user[1]

Optimal Time To Introduce Antivirus

These simulation results provides the knowledge about the impact of antivirus activities in network on virus spreading in network .

The graphs given below depicts the behaviour of code red worm . First graph shows the number of distinct IP address infected by worm second graph shows the similar observation in addition it gives graphical fitting against random constant spread model .

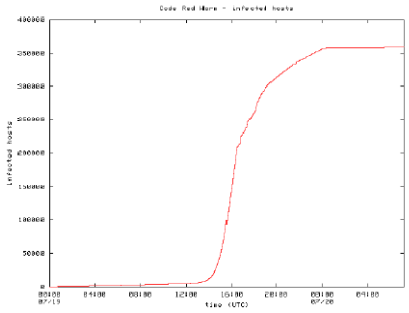

Fig. 2. The number of distinct IP addresses infected by Code Red v2 during its first outbreak [2,4]

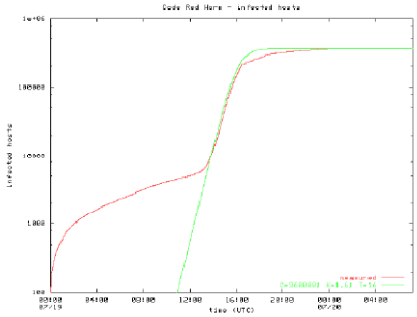

Fig. 3. The number of distinct IP addresses infected by Code Red v2 during its first outbreak, plotted on a log-log scale and fitted against the RCS model [2 ,4]

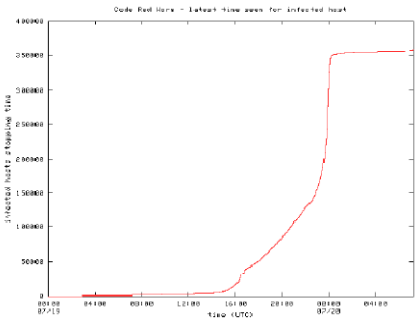

Fig. 4. Rate of \deactivation" of infected hosts [2,4]

Wireless sensor network security mechanism and network resource utilization have inverse in behavior there are various proposed scheme that get arrived in this direction.

There are various resource limitations in WSN[3]—

1. Energy limitations
2. Small memory
3. Low computation capability
4. Insecure nature

These limitations makes it tuff to make a strong defensive technique and WSN get suffer from various attacks like Denial of service attacks . Defensive measures that get developed uses various approaches to tackle the situation.

Intrusion detection schemes in wireless sensor network[3]----

1. Security protocol for sensor network
2. A security architecture for mobile WSN
3. Scalable session key construction protocol for WSN
4. A tree based approach for secure key distribution in WSN
5. A unified security framework with three key management scheme for WSN
6. A decentralized IDS for increasing security of WSN
7. A IDS for WSN
8. Anomaly Intrusion detection in WSN
9. Decentralized intrusion detection in WSN
10. Intrusion detection based security architecture for WSN
11. Energy efficiency of IDS in WSN
12. An improved IDS based on agent
13. A framework of machine learning based intrusion detection for WSN
14. Mobile agent based hierarchical IDS

Conclusion

In this paper we discuss the problem of viruses and show their impact on network by using graphical observations . The behaviour of viruses in network is shown with the help of state flow diagram and simulation results are discussed to study various spreading nature of viruses and defending nature of antivirus in network . Further The security limitations and defensive techniques in WSN are reviewed . Still a lot of work to be done in this domain .

15.

16.

References

[1] Xi Zhang and Krishna Chaitanya Tadi ," modeling virus and antivirus spreading over hybrid wireless adhoc and wired networks.

[2] Giuseppe Serazzi and Stefano Zanero ," Computer virus propagation models ".

[3] Surraya Khanum , Muhammad Usman and Ala Alwabel , " Mobile agent based intrusion detection system in wireless sensor network ".

[4] .Moore , D. , Shannon , C. Brown , J. : Code-red : a case study on the spread and victims of an internet worm . In the proceedings of the ACM.