International Journal of Soft Computing 7 (3): 131-134, 2012
ISSN: 1816-9503
© Medwell Journals, 2012

Double-Sticky-Honeynet for Defending Viruses in Computer Network

[1]Upendra Kumar, [2]Bimal Kumar Mishrav and [1]G. Sahoo
[1]Department of Information Technology, [2]Department of Applied Mathematics,
Birla Institute of Technology, Mesra, Ranchi, India

Abstract: The next generation computer viruses may spread within minutes to millions of host. A challenging task is to protect computer network from virus attacks. Researchers have developed a framework of computer network with honeynet using double honeypot and sticky honeypot. The double honeypot is used to recognize old and new viruses. The old virus gets filtered by router as well as updated antivirus installed in different hosts. Sticky honeypot attracts new virus to minimize transmission speed and redirect it towards unused IP address system. The Transmission Control Protocol (TCP) trick is implemented on unused IP address system having virus to make window size zero and further related system gets filtered by updated antivirus.

Key words: Honeypot, honeynet, double honeypot, sticky honeypot, router

INTRODUCTION

In the present scenario, secure on line data transmission is the basic necessity of computer network users which is not so easy, due to the attack of old and new viruses. To secure virus free data transmission several algorithms, anti viruses and network devices are developed even if virus free data transmission is not always true (Tirenin and Fantz, 1999; Cohen, 1987; Williamson and Leveille, 2003; Kumar and Navnit, 2007). Computer virus is software program either self generated or generated by Blackhat community to damage important files. It is transmitted through data into computer network and initially attacks on executable file and later on the whole system is damaged (Ytiser, 1993). Several algorithms have been developed to recognize viruses; one of them is Signature Based Intrusion Detection (Sommer and Paxon, 2003; Pouzol and Ducasse, 2002).

As researchers know, this technique has pre-defined signature so, this algorithm is unable to detect new virus attack. Another way to detect the attacked virus is Anomaly Based Intrusion Detection technique. In this approach the state of resources is to be conducted at an instance and capture huge profile (Kruegel and Vigna, 2003; Ghose *et al*., 1998; Kruegel *et al*., 2002). Since, the spread of malicious code is often an internet-wide event so, the fundamental difficulty is to detect unknown virus attack due to two reasons: firstly, Internet consist of large number of autonomous system that are managed independently that means coordinated defense system covering whole Internet is extremely difficult. Secondly, it is very hard to distinguish virus activity with normal activity, especially during initial phase of virus attack. These days concept of double honeypot has been implemented into computer network to detect old and new viruses. The double honeypot consists of inbound honeypot and outbound honeypot. An inbound honeypot attracts virus and transmit it towards outbound honeypot to record incoming threats for further analysis. The concept of sticky honeypot is used to minimize or remove virus from computer network having the property of low interaction honeypot. The old virus gets filtered by router and updated antivirus but the removal of a new virus attacks in the computer network still remains a challenges (Spitzmer, 2003; Jones and Romney, 2004; Tang and Chen, 2005, 2010; Yamoda *et al*., 2007). In this study, researchers have developed a frame researchers of computer network having double-sticky-honeynet. The honeynet uses double honeypot and sticky honeypot.

The double honeypot recognizes old and new viruses. The old virus gets filtered by router as well as updated antivirus while as new virus is recorded into outbound honeypot and redirected towards sticky honeypot. Sticky honeypot monitor unused IP address and then minimizes the attacking speed of virus and redirects the new virus towards unused IP address system. Several tricky Transmission Control Protocol

Corresponding Author: Upendra Kumar, Department of Information Technology, Birla Institute of Technology, Mesra, Ranchi, India

(TCP) options are implemented such as making windows size zero of an unused IP address system which contains viruses and then it gets filtered through updated antivirus. New generated virus may have properties of self replication and these types of viruses which does not get filtered. The unused IP address system is formatted.

BRIEF OVERVIEW OF HONEYPOT

Honeypots have emerged as a new technology with enormous potentiality for information security. The background of honeypot has been initiated by Cheswick (1997). Further this concept has been modernized by Stoll (2002). The developed honeypot has been continuously modified, evaluated and designed for implementations of different applications. The basic form of honeypots are designed to record IP address of hacker attacks, attract malicious code attack and recording malicious code attack for future study, etc. (Pouget and Holz, 2005). Initially, honeypots were used to divert attention of the attackers from the real network system so, that the hacker is unable to hack original data or information. Further, it has been extended to capture different type of new and old malicious codes.

Since, single honeypot is unable to detect, capture and remove several type of attacks on computer network so, the concept of honeynet has been developed. Honeynet is a tool that spans wide group of possible threats which define and analyze more information for detection, removal and future study (Provos, 2004).

Honeypots are categorized on the basis of their purpose as well as level of interactions (Lopez and Resendez, 2008; Marchese *et al*., 2011). On the basis of purpose, honeypots are divided into three categories: production honeypot, research honeypot and honey tokens. Whereas on the basis of interactions, honeypot is divided into the following three categories: low interaction honeypot, medium interaction honeypot and high interaction honeypot.

SYSTEM ARCHITECTURE

Three honeypots, i.e., an inbound honeypot, an outbound honeypot and a sticky honeypot together with gate translator and router are considered in the system architecture double-sticky-honeynet as shown in Fig. 1. The honeypot runs on specific system or on a virtual

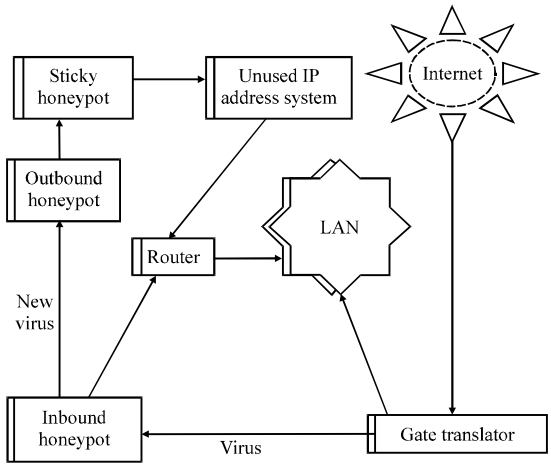

Fig. 1: Detection and removal of virus from computer network in double-sticky-honeynet architecture

computer simulated in the same computer. The gate translator is implemented at the edge router between local network and Internet. It is configured to recognize the list of unwanted port number during the process of data accession and as soon as viruses are found, connection is redirected towards inbound honeypot. The inbound honeypot easily attracts viruses and the related server implements Signature Based Intrusion Detection (SBID) algorithm to detect old viruses and its related packets and directs them towards router for filtration. The filtered data is transmitted towards the computer network where incoming packets are again filtered by updated antivirus through related host if required.

Further Position-Aware Distribution Signature (PADS) algorithm is implemented to verify new virus which gets attracted by outbound honeypot where it is recorded and analyzed and later on gets attracted by the sticky honeypot (Mokube and Adams, 2007; Hemraj *et al*., 2011). The sticky honeypot has the property of low interaction honeypot which minimizes the virus transmission speed and redirects it towards unused IP address system.

As viruses are forced to enter into unused IP address system, TCP tricks are implemented to make windows size zero and frequently updated antivirus is run on that system, even if some blocks of self replicated virus may not be removed. Still if some blocks of the virus are not removed by updated antivirus, researchers format the unused IP address system. The flowchart for virus detection and removal using honeynet is shown in Fig. 2.

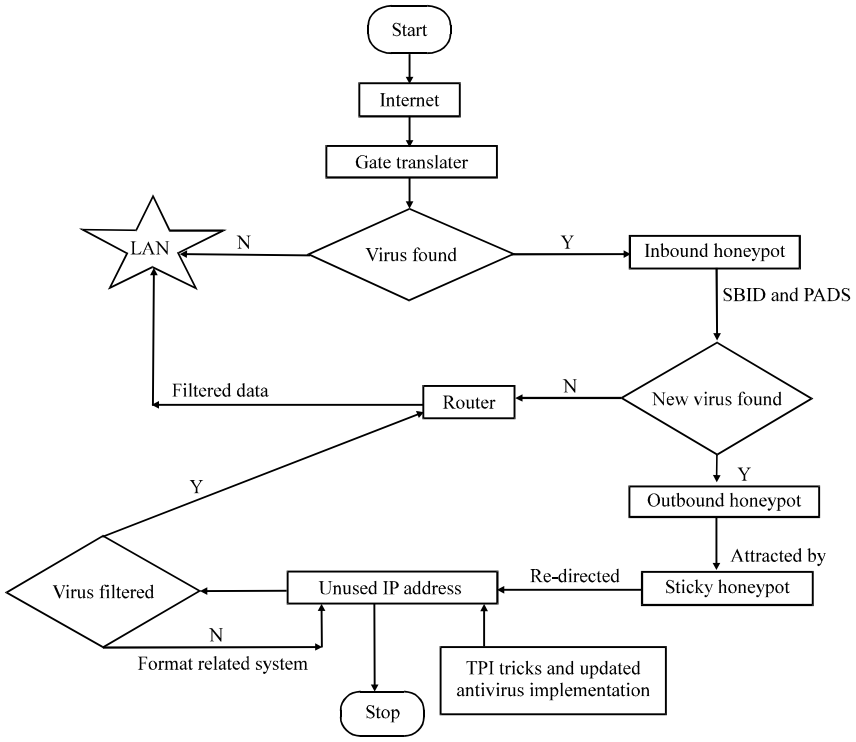

Fig. 2: Flowchart for virus detection and removal using honeynet

CONCLUSION

Researchers have developed virus free computer network using double-sticky-honeynet. Different types of honeypots have been defined and analyzed for different implications. The honeynet uses double honeypot and a sticky honeypot. The old and new viruses are detected by double honeypot using Signature Based Intrusion Detection and Position Aware Distribution Signature techniques. The old virus is filtered by router and updated antivirus, whereas new virus is removed by implementing sticky honeypot as well as TCP tricks and after that updated antivirus filters related system. Even if some blocks of new virus are left, they are removed by formatting the unused IP address system. The future research will concentrate on detection and removal of new virus with the help of new algorithm using sensor technique which can predict incoming virus and the related server can generate corresponding antivirus.

REFERENCES

Cheswick, W., 1997. An Evening with Berferd. In: Internet be Sized: Countering Internet Scuffles, Denning, D.E. and P.J. Denning (Eds.). ACM Press/Addison Wesley, New York, USA., pp: 103-117.

Cohen, F., 1987. Computer viruses: Theory and experiments. Comput. Security, 6: 22-35.

Ghose, A.K., J. Kanken and F. Charon, 1998. Detecting anomalous and unknown intrusions against programs. Proceedings of the 14th Annual Computer Security Applications Conference, December 7-11, 1998, Phoenix, AZ., USA., pp: 259-267.

Hemraj, S., M.B. Kumar and T.C. Panda, 2011. Extended honeypot framework to detect old/new cyber attacks. IJEST, 3: 2421-2426.

Jones, J.K. and G.W. Romney, 2004. Honeynets: An educational resource for I.T Security SIGITE. Salt Lake City, Utah.

Kruegel, C. and G. Vigna, 2003. Anomaly Detection of Web based Attacks. ACM Press, New York, USA., pp: 251-261.

Kruegel, C., T. Toth and E. Kirda, 2002. Service specification anomaly detection for network intrusion detection. Proceedings of the Symposium on Applied Computing, March 10-14, 2002, Madrid, Spain.

Kumar, M.B. and J. Navnit, 2007. Fixed period of temporary immunity after run of anti malicious software on computer nodes. Applied Math. Comp., 190: 1207-1212.

Lopez, M.H. and C.F.L. Resendez, 2008. Honeypots: Basic concepts, classification and educational use as resource in information security and course. Proceedings of the Information Science and IT Education Conference, (IITEC'08), Mexico, pp: 69-76.

Marchese, M., R. Surlinelli and S. Zappatore, 2011. Monitoring unauthorized Internet access through honeypot system. Int. J. Commun. Syst., 24: 75-93.

Mokube, L. and M. Adams, 2007. Honeypot: Concepts, Approach and Challenge. ACMSE, Winston-Salem, North Carolina, USA, pp: 23-24.

Pouget, F. and T. Holz, 2005. A Pointillist Approach for Comparing Honeypot. In: Intrusion and Malware Vulnerability Assessment, Julisch, K. and C. Krugel (Eds.). Springer, Berlin/Heidelberg, Germany.

Pouzol, J.P. and P. Ducasse, 2002. Formal specification of intrusion signatures and detection rules. Proceedings of the 15th IEEE Workshop on Computer Security Foundations, June 24-26, 2002, Nova Scotia, Canada, pp: 64.

Provos, N., 2004. A virtual honeypot framework. Proceedings of the 13th USENIX Security Symposium, August 9-13, 2004, San Diego, CA., USA.

Sommer, R. and V. Paxson, 2003. Enhancing byte-level network intrusion detection signatures with context. Proceedings of the 10th ACM Conference on Computer Communication Security, October 27-30, 2003, Washington, DC., USA., pp: 267-271.

Spitzmer, L., 2003. Open source honeypots: Learning with honeyd. http://www.net-security.org/news.php?id=1855.

Stoll, C., 2002. The Cuckoos' Egg: Tracking a Spy Through the Maze of Computer Espionage. 1st Edn., Pocket Books, New York, USA.

Tang, Y. and S. Chen, 2005. Defending against internet worms: A signature-based approach. Proceedings of the IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, Volume 2, March 13-17, 2005, Miami, FL., USA., pp: 1384-1394.

Tang, Y. and S. Chen, 2010. Defending against Internet Worms: A Signature based Approach. Department of Computer and Information Science and Engineering, University of Florida, Gainesville, FL., USA., pp: 32611-32620.

Tirenin, W. and D. Fantz, 1999. A concept for strategic cyber defense. Proceedings of the Conference on Military Communication, Volume 1, October 31-November 3, 1999, Atlanta City, New Jersey, pp: 458-463.

Williamson, M.M. and J. Leveille, 2003. An epidemic logical model of virus spread and clean up. Hewlett-Packard Laboratories, Bristol. http://www.hpl.hp.com/techreports/2003/HPL-2003-39.pdf.

Yamoda, Y., T. Katoh, B.B. Bista and T. Takata, 2007. A new approach to early detection of an unknown worm. Proceedings of the 21st International Conference on Advance Information Networking and Application Workshops, Volume 1, May 21-23, 2007, Niagara Falls, Canada, pp: 194-198.

Ytiser, T., 1993. Polymorphic viruses: Implementation, detection and protection. VJDS, Advance Centre Research Group. http://ivanlef0u.fr/repo/madchat/vxdevl/vdat/pviripd.htm.