International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 1 [ISSN : 2250-3757]
Publication Date : 30 April, 2015

An Agent-oriented Website Sucurity System

Yanlong Zhang

***Abstract* — This paper demonstrates a multi-agent solution to website security management. The results of preliminary use of the software tool are inspiring. The model described provides a generic architecture. With addition of mobile agents and neural network knowledge base model, the model can be extended and performs more effectively and efficiently in website security and forensic analysis.**

Keywords — network security, forensic analysis, intrusion detection, intrusion prevention, agent-oriented system, multi-agent system

I. Introduction

In today's generation, the internet is viewed as a vital part of any sort of communication. From e-mails and chatting to shopping and internet banking, the services provided over the internet are ever evolving. However the attacks conducted on the internet are also growing simultaneously.

One of the attacks is to change the website content maliciously, such as publishing a fake notice on a popular website or changing a picture on the homepage.

In order to address such issues, investigating how this happened, who did it, how to prevent it to happen again, etc., network circles have continued to develop new technologies, techniques and tools.

II. Related Research

Network forensics identifies suspicious entities in a cyber attack and performs step-by-step reconstruction of the attack by using evidence obtained from the networked environment, such as server log files. Detection of the primary evidence is the starting point for any forensic investigation [1, 2]. Primary evidence refers to information that directly indicates attack or security violation and is detected from an intruding detection system (IDS). IDS is viewed as network's burglar alarm, and process of monitoring the event occurring is of prime importance [3].

Intrusion prevention system (IPS) is triggered after IDS to resolve ambiguities in passive network monitoring by placing detection system on the line of attack [4].

The next innovation is the combination of IDS and IPS, as intrusion detection and prevention system (IDPS) [4]. Radack in [3] pointed out that as investigating activity is so frequent on the internet, investigation detection should be performed primarily on the key pages, in the internal networks.

Dr. Yanlong Zhang
Manchester Metropolitan University
UK

There exist several methodologies and approaches in network forensic researches, such as correlation method and predefined attack scenarios [5], Novel based graph approach [1], soft computing based frameworks [6, 7], forensic process models [8, 9, 10, 11]. These models presented a clear direction in detection and prevention.

When it comes to cyber attack, such as hacking, DOS, IP spooling, the main source to determine who conducted the attack is located in the attacker's IP address and this is why IP trackback is of major importance in network forensic analysis [12]. The major techniques can be referred to [13, 14, 15, and 16].

The approaches and techniques discussed above have truly addressed the issues of intrusion in general. However, the intruders or hackers are adopting new techniques as well. For example, they can falsify the IP packet dynamically, and/or falsify server log file, etc. [17, 18].

III. Our Approach

The development of distributed computing environment has stimulated agent technologies. Agents are able to complete complicated tasks automatically and cooperatively [19]. A multi-agent system, in which agents collaborate with other agents, is utilised. In this paper, we use a master-slave multi-agent model [20] to build an agent-oriented website security system (AOWSS), where a master agent controls, commands, and delegates tasks to a number of slave agents. Agents collaborate with each other under the control of the master, to complete their tasks. The master should ensure there are no negative interactions between the activities of the slaves, and to achieve the goal of the system.

The AOWSS contrasts with traditional forensic system which can be used only after a hazard had caused serious damages. The AOWSS can monitor the website visitors' behaviour in real-time and stop any hazard to happen. In addition, it will further investigate the issue, such as blocking a potential hacker from further damage, locating a potential hacker and presenting a report. The framework is shown in Figure 1.

A. Managing Agent

The managing agent is the master of the multi-agent system. It receives information from other agents, makes decisions using the knowledge base, and sends instructions to other agents.

B. Knowledge Base

The knowledge base stores knowledge which is extracted from information bases. It is a structured representation of the information bases. The knowledge depicts the syntactic and semantic information, and is shared among the agents.

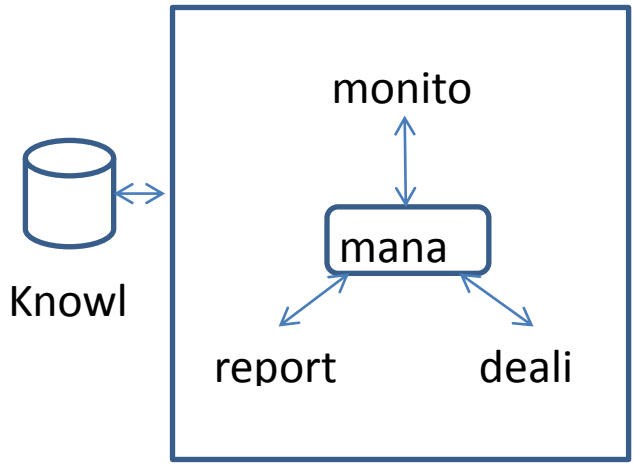

Figure 1. A general architecture of AOWSS

Currently the knowledge base uses a traditional data dictionary model. We wish to upgrade it to an artificial neural network model in the future.

C. *Monitoring Agent*

The monitoring agent scans key pages of the website 24/7. We currently set the frequency as once per minute. With our preliminary results, the frequency can be set as fast as once per 3 seconds. It can be configured depending on the computing speed and the size of website monitored. We use MD5 to create a fingerprint for each key page. The monitoring agent will be alarmed when any fingerprint is changed, and sending the error page ID to the managing agent.

D. *Dealing Agents*

The dealing agents receive instructions from the managing agent. Currently our dealing agents complete three types of tasks: recovering the changed webpage; blocking the potential hacker, and tracing the potential hacker.

E. *Reporting Agent*

The reporting agent receives information from the managing agent. With the aid of the knowledge base, it produces a readable report, rather than a-thousand-line log file, for the client.

IV. Development and Application of a software tool

A software tool was implemented using JAVA. We tested our tool on some data-sensitive systems. We will present a case in this section.

At 11:29 am, on 29 April 2014, one suspected hacker tried to change some contents on the homepage of a website we monitored.

When the MD5 digit of the homepage was changed, the monitoring agent triggered the alarm. One dealing agent undid the changes on the same minute.

All incoming IP addresses remaining on that minute were recorded as suspects.

11:32 second attempt was made to change the homepage. This time the managing agent was able to reduce the scope of suspected IPs.

One dealing agent recovered the changes, while another dealing agent started to trace the suspected IPs.

On 30 April, the hacker's IP was confirmed after its fifth attack. After trackback of IP completed, the report showed that the IP address was a fake IP obtained from a HideYourIP site. The IP address was blocked.

V. Conclusion

This paper demonstrates an agent-oriented solution to website security management. The model described provides a generic architecture. With addition of the application of mobile agents and neural network knowledge base model, the model can be extended and perform more effectively and efficiently in website security and forensic analysis.

After six months testing, we find the following improvement points.

1. Using artificial neural network to model the knowledge base. With the rapid increase of data gathered, querying time is lengthened. A more efficient data handing model should be applied.

2. Using mobile agent for dealing agents design.

References

[1] W. Wang and T.E.Daniel, "A graph based approach towards network forensic analysis," ACM Trans. Information System Security, 12(1), article 4, 2008.

[2] E.S.Pilli, R.C.Joshi and R.Niyogi, "Data reduction by identification and correlation of TCP/IP attack attributes for network forensics,"Proc. International Conference and Workshop on Emerging Trends in Technology, 2011.

[3] S.Radack, Intrusion Detection and Prevention System, National Institute of Standards and Technology, 2007.

[4] K.Scarfone and P..Mell, Guide to Intrusion Detection and Prevention Systems, National Institute of Standards and Technology, 2007.

[5] X.Qin amd W.Lee, "Discovering novel attack strategies from infosec alerts," Proc. 9th European Symposium on Research in Computer Security, 2004.

[6] Z. Liu and D.Feng, "Incremental fuzzy decision tree-based network forensic system," Proc. International Conference on Computational Intelligence and Security, 2005, pp.995-1002.

[7] N.Liao, S.Tian and T.Wang, "Network forensic based on fuzzy logic and expert system," Computer Communications, Vol. 32, No. 17, 2009, pp.1881-1892.

[8] J.P.Craiger, "Computer forensics procedures and methods," in H.Bidgoli(ed.), Handbook of Information Security, John-Wiley, 2006.

[9] E.S.Pilli, R.C.Joshi and R.Niyogi, "Network forensic frameworks: survey and research challenges," Digital Investigation, 7, 2010, pp.14-27.

[10] Y.Yusoff, R.Ismail and Z.Hassan, "Common phases of computer forensics investigation models," International Journal of Computer Science and Information Technology, Vol. 3, No. 3, 2011.

[11] M.Pollitt, "Computer forensics: an approach to evidence in cyberspace," Proc. National Information Systems Security Comference, Vol. II, 1995, pp. 487-491.

[12] C.Gong and K.Sarac, "A More Practical Approach for Single-Packet IP Traceback using Packet Logging and Marking, " IEEE Trans. On Parallel and Distributed System, Vol. 19, No. 10, 2008, pp. 1310-1324.

[13] N.Meghanathan, S.R.Allam and L.A.Moore, "Tools and techniques for network forensics," International Journal of Network Security and Its Applications, Vol. 1, No. 1, 2009.

[14] O.Demir, P.Ji and J.Kim, "Session Based Packet Marking and Auditing for Network Forensics," IJDE, 2007.

[15] S.Mitropoulos, D.Patsos and C.Douligeris, Network Forensics:Towards A Classification of Traceback Mechanisms, IEEE, 2005.

[16] B.Carrier and C.Fields, "The session token protocol for forensics and traceback," ACM Trans. On Information and System Security, Vol. 7, No. 3, 2004, pp.333-362.

[17] J.Haas, "Tripwire," http://linux.about.com/cs/linux101/g/tripwire.htm, accessed 29 June 2014.

[18] M.Tang and C.Fidge, "Reconstruction of falsified computer logs for digital forensics investigation," CRPIT, Vol. 105, 2010.

[19] M.Wooldridge, J.PMuller abd M.Tambe, Intelligent Agents II: Agent Theories, Architectures, and Languages, Springer, 1996.

[20] D.T. Ndumu and H.S.Nwana, "Research and development challenges for agent-based system", IEEE proc. Software Engineering, Vol.144, No.1, 1997.

About Author (s):

Yanlong Zhang received his Ph.D from Oxford Brookes University in 2005. He is currently a senior lecturer in the School of Computing, Mathematics and Digital Technology, Manchester Metropolitan University. His research interests include website usability, website security and computer forensics.