The Development of Agent Information for Intrusion Detection

Bambang Sugiantoro
Dept. of Informatics, State Islamic University Sunan Kalijaga, Yogyakarta.
bambang.sugiantoro@uin-suka.ac.id

Abstract

As the challenges and problems surround intrusion rises rapidly, the intrusion detection system has been gradually developed. Agent-based approach for intrusion detection system has developed from single to multi agent, and later developed mobile agents in order to increase system's capability to face with a more complex challenge and change. A number of studies had been identified that mobile agent can reduce network traffic, however the study related to intrusion detection using static and mobile agent for finding intruder has not been fully achieved.

Keywords: *Information, Intrusion, mobile, networks*

1. INTRODUCTION

Along with the development of the Internet network, crimes committed in cyberspace experiencing growth. According to data from the annual report 2013 panda lab reported infiltration associated with illegal acts to login in social networks, especially Twitter by 250,000 [1]. Non-material and material loss is the impact that causes the illegal acts committed by an intruder. Research in the field of security to detect intruders becomes important to get attention, because of losses caused by the intrusion. Infiltration / intrusion defined activities that seek to damage or misuse the system or any business that do compromise the integrity, trustworthiness or availability of a computer's resources. This definition does not depend on the success or failure of the action, so it relates to an attack on a computer system [2].

Mobile Agent provides a solution to be implemented in the network because it uses relatively little bandwidth compared to conventional client-server concept, the mobile agent traveled to resources so as to reduce network traffic. Another advantage of the mobile agent is its ability to survive and operate even though its owner had dropped out of the network. This makes the concept of mobile agent is superior to the conventional model of client server

Approaches mobile agent system for intrusion detection in multi host, has the advantage to improve performance IDS is, when the mobile agent is applied has several drawbacks, among is the issue of security vulnerabilities of mobile agent of the problems and code size mobile agent IDS, potential threats can be categorized into four , the agent of the mobile agent, agent to the visited mobile agent platform, the platform of the mobile agent and entities external to the platform [3]. In the proposed research to improve the intruder issues including external entities that take advantage of the departure of the mobile agent to conduct infiltration.

2. DESCRIPTION OF INTRUSION DETECTION ARCHITECTURE

General architectural of mobile agent to IDS with the cooperation mechanism between multi agent and to take advantage of misuse detection IDS analysis with string matching technique. The set of hosts to be detected is {h1, h2, h3, ..., hk}, with D data set obtained is {d1, d2, d3, ..., dk}. Mobile agent

(agent slave) which created of host origin, will perform intrusion detection on each of these hosts, then will return to the originating host h0. Data obtained by the mobile agent (agent slave) will increase along with increasing host has been detected. The set itinerary mobile agent (agent slave) is {h0, h1, h2, h3, ..., hk, h0}. After executing in all host intrusion detection, mobile agent (agent slave) will be returned to the originating host h0, information detection results obtained is {d1, d2, d3, ..., dk}.

When the mobile agent (agent slave) has finished detecting intrusion in h1, agents slave asking for help to agents static (master agent) to be sent auxiliary agents to be placed in h1, then the agent static (master agent) sends the mobile agent (agent clone) to h1 , After the mobile agent (agent slave) move on to the next host. This mechanism is repeated until the last host hk. Mobile agent (agent clone) hk amount will be made to help the mobile agent (agent slave). In case of infiltration of each mobile agent (clone agent) will send the detection result to static agents (master agent) to appear as a result of intrusion detection.

3. ANALYSIS OF INTRUSION DETECTION ARCHITECTURE

Use case diagrams mobile Agent describes the main processes of the analysis of the functional requirements made by the model are respectively the processes (i) the itinerary mobile agent (itinerary), (ii) the process of intrusion detection by the mobile agent, and (iii) intrusion detection information. Tests conducted on five computers on a local network with the following configuration: (i) a single computer as the originating host with the IP address 192.168.231.1 windows operating system, MySQL database server, Aglets SDK and JDK. (ii) as a host computer that will be the first destination IP address 192.168.231.18 detected by the Windows operating system, Aglets SDK and JDK. (iii) host as the destination computer that will be detected by the IP address 192.168.231.17 linux operating system, Aglets SDK, JDK and OSSEC HIDS. (iii) host as the final destination computer that will be detected by the IP address 192.168.231.24 Linux operating system, Aglets SDK, JDK and OSSEC HIDS. (v) 192 168 231 180 IP computer as an intruder

Communication between the master agent with the mobile agent using the standard KQML (Knowledge Query and Manipulation Language). Mobile agents are implemented using aglet. JKQML used Aglet using communication and exchange messages. Implementation in the exchange of messages between master agent with the mobile agent using a proxy. Arguments message sent from the master agent to the mobile agent or otherwise in the form of arguments that can be serialized, by implementing the java.io.Serializable. Messages sent in the form of an object. Object recognizable messages of its kind (kind). This string property is used to distinguish between a message with another message. Object messages can also be an optional argument fatherly data associated with a particular message, arguments can be either atomic argument of type string, integer, and other data types or tabular form hash table. In manage the message came, the master agent and mobile agent using a method handle message.

The components of the agent in terms of the resulting size is as follows: 9:31 size AgletMaster.java have KB (9.539 bytes), AgletCloned.java has a size of 5.71 KB (5,848 bytes) and measuring 3.66 AgletSlave.java KB (3.749 bytes) can be found at table 6.4. Size relatively small mobile agent makes it possible to roam with nimble on computer networks, this is one of the factors did not consume high bandwidth. Different test has been carried out between the two types of mobile agent: slave agents and agents clone, more detail can be found in the appendix. Test equipment used: Mann Whitney test (non-parametric test) commensurate with T test. Basis for decision making Ho is rejected if the value Asymp. Sig> 0.05 (95% confidence level). Looks sig. = 0.037 <0.05. It means Ho is rejected (h1 accepted). There are differences between the two mobile agent bytes, wherein Clone Agent tend to be larger than the results of the experimental agent Slave

Comparison shows that the mobile agent and mobile agent slave clone in terms of bandwidth consumption is smaller than DIDMA. Performance indicators show managed to improve performance doctoral research in the aspect of bandwidth consumption. This is because in the design of mobile agent using computing resources to be charged on each host being visited and the complexity of the algorithms used linear category.

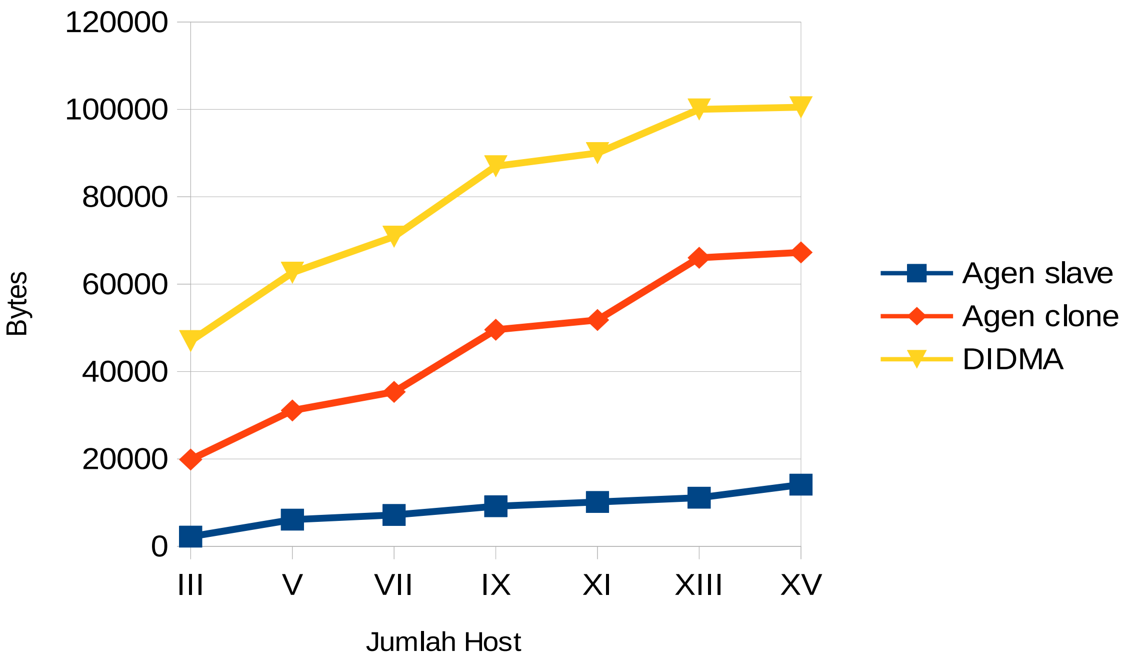

FIGURE 1 Bandwidth Mobile agent

The average execution time mobile agent clone is 315 seconds while the average execution time DIDMA 300 seconds for the number of hosts 3. Then the number of hosts: 5, 7, 9, 11, 13 and 15 have a clone for mobile agent execution time: 525 seconds , 735 seconds, 945 seconds, 1155 seconds, 1365 seconds and 1575 seconds. While DIDMA execution time: 500 seconds, 700 seconds, 900 seconds, 1100 seconds, 1300 seconds and 1500 seconds. From the resulting data can be analyzed that the execution time between the mobile agent DIDMA clone does not mean for a relatively small number of hosts. Research DIDMA faster than the mobile agent clones generated. This is because the double traffic occurs on the detection system that uses cloning. But the speed of the mobile agent slave faster than DIDMA and mobile agent clone.

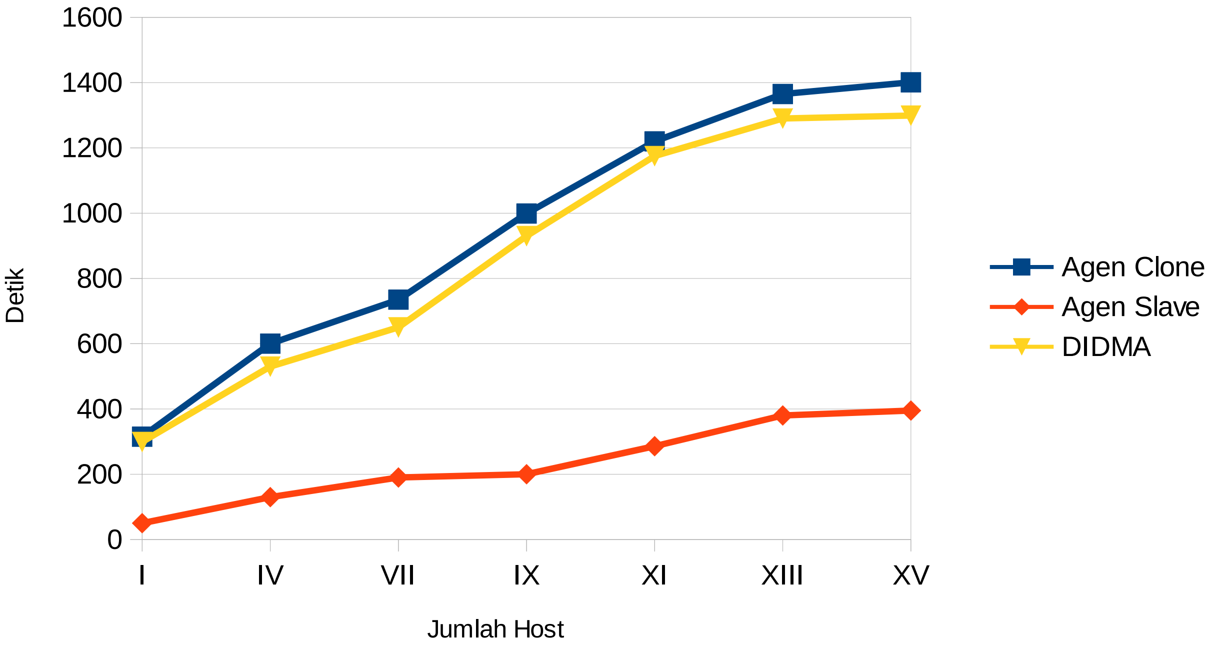

FIGURE 2 Execution Time

The average bandwidth usage of mobile agent while the clone is 19 854 bytes of bandwidth usage DIDMA: 50000 bytes for the number of hosts number 3. Then the number of hosts: 5, 7, 9, 11, 13 and 15 for mobile agents clone had average bandwidth usage : 33 090 bytes, bytes 46 326, 59 562 bytes, bytes 72 798, 86 034 bytes and 99 270 bytes. While the average bandwidth usage DIDMA: 60000 bytes, 70000 bytes, 80000 bytes, 90000 bytes, 10000 bytes and 110000 bytes. From the resulting data can be analyzed that the average bandwidth usage between mobile agent clone DIDMA with a very significant amount of variation in different hosts. Prototypes mobile agent models for intrusion detection related to potential intruders who take advantage of the departure of the mobile agent and the agent component with the focus of this cooperation mechanism is practically quite realistic, but there are some aspects still need to be developed further. Below is given the advantages and disadvantages of the prototype has been built and for further research work.

4. CONCLUSION

Prototype models of mobile agent for the resulting intrusion detection has been proven superior in terms of bandwidth usage, especially compared DIDMA clone mobile agent, but on aspects of mobile agent clone execution time is lower than previous studies. Prototypes model of mobile agent for the detection of intrusion by considering the potential intruder's departure that utilize mobile agent has been successfully developed to provide intrusion detection information. The information represents the aspect of integrity in this case the gap port has been opened by an intruder and information that represent aspects of authentication in this case regarding the illegal login. There is a static agent is the master agent and the two mobile agent: slave agents and agents clone. Utilization techniques used string matching detection process analysis slave mobile agent that has been built and able to carry out their duties properly interact. The ability of the agent contained in the chapter on the design of the model also has the ability multi agent. Prototype appropriate and meets the specification requirements that have been established, as demonstrated by the achievement of the following results: (i) the mobile agent itinerary (itinerary), (ii) the process of intrusion detection by mobile agent, and (iii) intrusion detection information.

REFERENCES

[1] Pandalabs., 2014, Annual Report Pandalabs 2013 Summary, Panda security, USA

[2] Patil, N., Das, C., Patankar, S. and Pol, K., 2008, Analysis of Distributed Intrusion Detection System Using Mobile Agent, First International Conference on Emerging Trends in Engineering and Technology, India, 16-18 July 2008

[3] Prymek, M. and Horak, A, 2008, Using KQML as the Agent Message Content Language in an Electrical Power Network Simulation, Vaclav Snasel, Znalosti

[4] Roesch, M., 1999, Snorth Lightweight Intrusion Detection System for Network, In Proceedings of USENIX (LISA'99), Country, Month 1999

[5] Safuan, H., Cheah, Z., lim, H. and Chin, J., 2005, Intrusion Detection System based on Mobile agent, 1st International Conference on Computers, Communications, & Signal Processing with Special Track on Biomedical Engineering, Kualalumpur, 14-16 November 2005

[6] Sahota, R., Chauhan, A. and Suneja, P., 2013, A Novel Approach for Introducing Advanced Security in Mobile Agents, International Journal of Advances in Computer Networks and its Security, 2, 3, 139-143

[7] Saleh, K. and El-Morr, C., 2004, M-UML: An Extension to UML for The Modelling of Mobile Agent-Based Software System, Information and Software Technology by Science Direct, 6, 4, 219-227

[8] Sharma, S., 2011, A Survey on Different Security Techniques of Mobile Code, International Journal of Engineering and Advanced Technology, 1, 1,

[9] Singh, M. and Sodhi, S., 2007, Distributed Intrusion Detection using Aglet Mobile Agent Technology, Proceedings of National Conference on Chalenges & Opportunities in Information Technology, India, 23 March 2007

[10] Spaford, E.H. and Zamboni, D., 2000, Intrusion Detection Using Autonomous Agents, Computer Networks: The International Journal of Computer and Telecommunications Networking, 4, 34, 547-570

[11] Straber, M., Rothermel, K. and Maihofer, C., 1998, Providing Reliable Agent for Electronic Commerce , Proceedings of Trends in Distributed System For Electronic Commerce (TREC'98), Germany, June 1998

[12] Wang, H., Wang, Z., Zhao, Q. Wang, G., Zheng, R. and Liu, D., 2006, Mobile Agents for Network Intrusion Detection Resistance, In Proceedings of The International Workshops on Advanced Web and Network Technologies, and Application, Harbin China, Month 2006

White, G.B., Fisch, E.A. and Pooch, U.W. , 1996, Cooperating security managers: a peer-based intrusion detection system, Network IEEE, 1, 10, 20-23