International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

Distributed Intrusion Detection System Using Mobile Agent Technology

Kajal K. Nandeshwar, Komal B. Bijwe

Department of Computer Science and Engineering, P. R. Pote (Patil) College of Engineering, Amravati, India

kajal.nandeshwar.02@gmail.com , 9420304508

Abstract— The one of the most serious threats to computer security is the unauthorized intrusion into a computer system or network. Due to the rapid growth of the network application, new kinds of network attacks are emerging endlessly. The distributed intrusion detection systems detecting the intrusion activity spread over the network. A distributed intrusion detection system may need to deal with different audit record format. The mobile agents are captures the audit records and are best suited for remote information retrieval. The distributed intrusion detection system used mobile agents which defends a distributed collection of hosts supported by a LAN or internetwork.

Keywords— Intruders, IDS, DIDS, DIDSMA, Mobile Agent, LAN, Attack

INTRODUCTION

The several hosts are connected by a network and the intruders attack on the several computing nodes and may move between several nodes in the network [1]. The IDS defines to be the problem of detecting individual who are unauthorized user of a computer system [6]. The IDS which identify computer system intrusions and misuse by collecting and analyzing data mainly focus on single system, however the DIDSMA is proposed which consisting of a multiple IDS over a large network. The DIDSMA uses the set of software entities known as mobile agents that can move between one node to another node within a network. Mobile agents are provides a new and useful paradigm for distributed computing and capable of suspending processing on one platform and moving onto another where they resume execution of their code [7]. DIDS that combines distributed monitor at every host and data reduction with the centralized data analysis to monitor heterogeneous network of computer [6].

WEAKNESSES IN EXISTING SYSTEM

Traditional IDS have a central coordinator with a static hierarchical architecture, which indicate the failure of existing of single point and hierarchy vulnerability [3]. The DIDS were introduced to overcome this susceptibility where mobile agents are considered in the implementation of such technology to play a prominent role [9].

- Limited flexibility: For the specific environment, IDS have typically been written.
- Limited response capability: IDS have traditionally focused on identify attacks.
- High number of false positive: False alarms are high and recognization of attack is not perfect.

RELATED WORK

A. DIDS

A number of IDSs have been proposed for a networked or distributed environment. Early systems included ASAX [11], NSTAT [12]. These systems require the audit data collected from different places to be sent to a central location for an analysis. NetSTAT [13] is another example of such a system. In NetSTAT attack scenarios are modeled as hyper graphs and places are probed for network activities. Although NetSTAT also collects information in a distributed manner, it analyses them in a central place. The scalability of such systems is limited due to their centralized nature. To improve scalability later systems such as EMERALD [14], GriDS [16] and AAFID [15], deployed instruction detection systems at different locations and organized them into a hierarchy such that low-level IDSs send designated information to higher level IDSs. EMERALD uses both misuse detection and statistical anomaly detection techniques. This system employs a recursive framework, which allows generic components to be deployed in a distributed manner [14]. To detect intruders, GriDS aggregates computer and network information into activity graphs which reveal the causal structure of network activity [16]. AAFID consists of agents, filters transceivers and monitors organized in a tree structure [15]. DIDS are simply a superset of the conventional IDS implemented in a distributed environment.

DIDS Architecture

DIDS consist of three different components: a single host monitor per host, a single LAN monitor for each broadcast LAN segment and a system director [4].

The overall architecture of DIDS consisting three main components which are as follows:

- **Host agent module:** An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security related events on the host and transmit these to the central manager.
- **LAN monitor agent module:** Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager,
- **Central manager module**: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion [2] - [8].

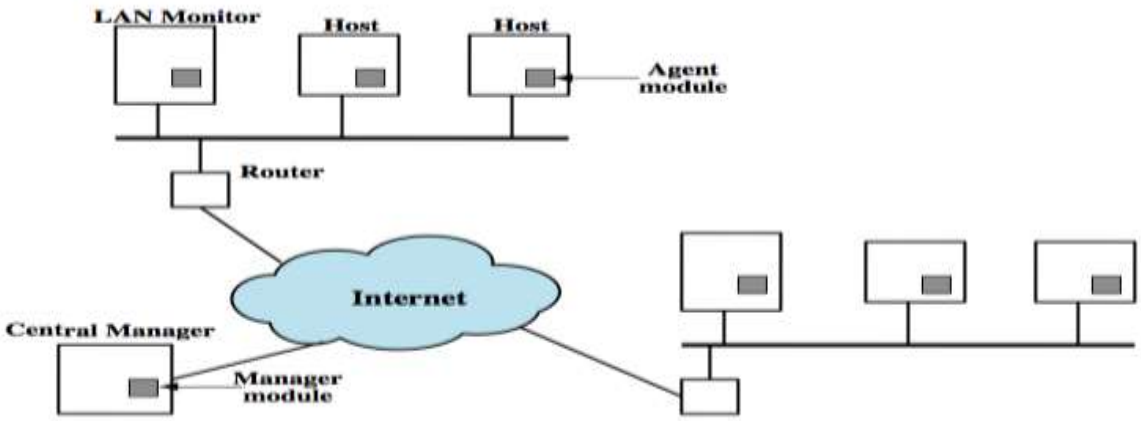

Fig1: Architecture for Distributed Intrusion Detection System

A. Introduction to mobile agent

Mobile agent is a composition of computer software and data which is able to migrate from one computer to another autonomously and continue its execution on the destination computer [3].Mobile agent technology can potentially overcome a number of weaknesses, intrinsic to existing IDSs that employ only static components [7].The intelligent agents for intrusion detection project [10], have developed IDS using distributed multiple layers of lightweight intelligent mobile agents that apply data mining techniques to detect intrusions.

Fig2 illustrate the architecture of mobile agent.

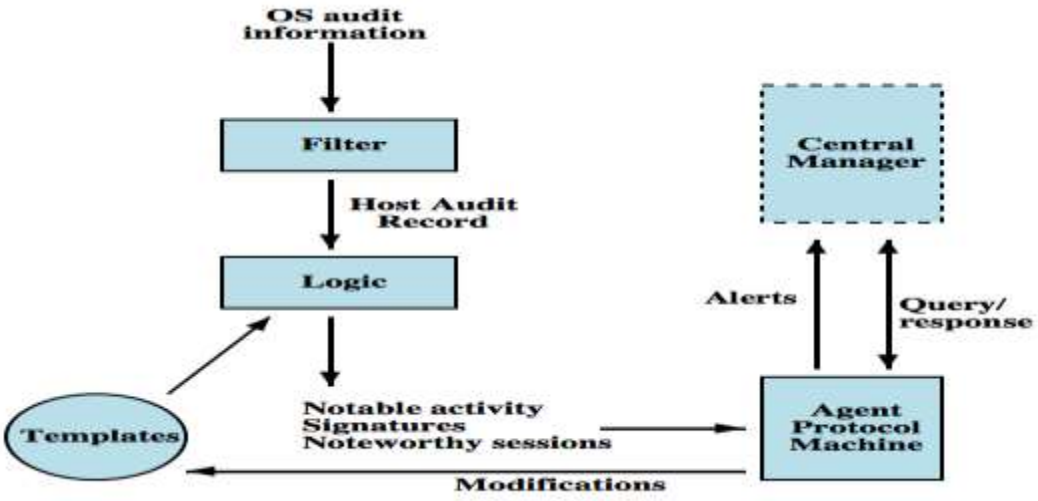

Fig2: Mobile Agent Architecture

The native audit collection system produced each audit record produced by the agent. A filter is applied that retains only those records that are of security interest. These records are then reformatted into a standardized format referred to as the host audit record (HAR).

Next, a template-driven logic module analyzes the records for suspicious activity. At the lowest level, the agent scans for notable events that are of interest independent of any past events. Examples include failed file accesses, accessing system files, and changing a file's access control. At the next higher level, the agent looks for sequences of events, such as known attack patterns (signatures). Finally, the agent looks for anomalous behavior of an individual user based on a historical profile of that user, such as number of programs executed, number of files accessed, and the like. An alert is sent to the central manager when suspicious activity is detected. The central manager may query single systems for copies of HARs to correlate with those from other agent. The LAN monitor agent also provides data to central manager and audits host-host connections, service used [2] - [8]. There are multiple attacks are implemented. The Fig3 shows the result. The database stores the history of all nodes [1].

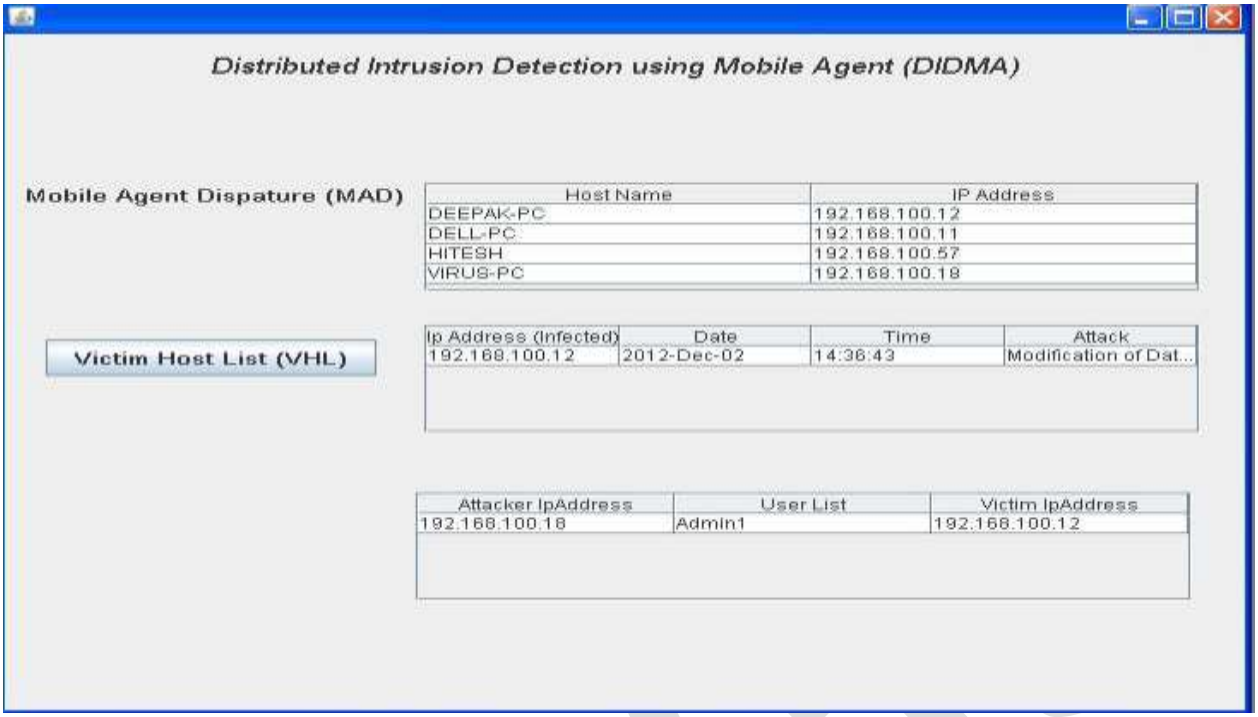

Fig3: Distributed intrusion detection using mobile agent

CONCLUSION

The DIDSMA are offers a foundation for a machine independent approach that can expand from stand alone intrusion detection to a system which can be correlate activity from a number of sites and networks to identify malicious activity that would remain undetected. Use of mobile agents in DIDSMA makes application advantageous such as it reduces load of network. Mobile agents are more realistic and can find intruder in distributed system and take action against malicious activities. DIDSMA are flexible and provides facilities and advantages which are beneficial. DIDMA can be easily extended to detect new attacks by adding new MAs.

REFERENCES:

[1] Trushna T. Khose Patil, C.O.Banchhor," Distributed Intrusion Detection System using mobile agent in LAN Environment", Department Of Information Technology ,SCOE, Pune, India, Assistant Professor Department Of the Information Technology, SCOE, Pune, India, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 4, April 2013.

[2] Willium Stallings, Network Security Essentials: Applications and Standards, 4th ed, Pearson Education, Inc., 2011, pages 305-322.

[3] Kamaruzaman Maskat, Mohd Afizi Mohd Shukran, Mohammad Adib Khairuddin & Mohd Rizal Mohd Isa, "Mobile Agents in Intrusion Detection System: Review and Analysis", Faculty of Science and Technology Defense, Department of Computer Science, National University Defense University of Malaysia, Sungai Besi Camp 57000 Kuala Lumpur, Malaysia.

[4] James Brentano, Steven R. Snapp, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt, Biswanath Mukhargee, Stephen E. Smaha, "An Architecture for a Distributed Intrusion Detection System", Division of Computer Science, university of California, Davis, California 95616.

[5] Abhijit Dwivedi, Y. K. Rana, B. P. Patel," A Literature Review on Agent Based Intrusion Detection System, "Department of CSE Department of CSE Department of the CSE REC, Bhopal (M.P), India REC, Bhopal (M.P), India REC, Bhopal (M.P), India, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014 ISSN: 2277 128X.

[6] Steven R. Snapp, James Brentano, Gihan V. Dias, Terrance L. Goan, L. Todd Heberlein, Che-Lin Ho, Karl N. Levitt, Biswanath Mukherjee, Stephen E. Smaha, Tim Grance, Daniel M. Teal, and Doug Mansur,"DIDS (Distributed Intrusion Detection System) -Motivation, Architecture and An Early Prototype", Computer Security Laboratory Division of Computer Science, University of California, Davis, Davis, California 95616.

[7] Wayne A. Jansen, "Intrusion Detection with Mobile Agents", National Institute for Standards and Technology Gaithersburg, MD 20899.

[8] Mr. Suryawanshi G.R. Prof. Vanjale S.B," Mobile Agent for Distributed Intrusion detection System in Distributed System", B.V.U.C.O.E, Pune, International Journal of Artificial Intelligence and Computational Research (IJAICR.) ", Jan -June 2010, ISSN-0975-3974.

[9] M. Eid, "A New Mobile Agent-Based Intrusion detection System Using distributed Sensors", Inproceeding of FEASC, 2004.

[10] G. Helmer, J. Wong, Y. Wang, V. Honavar, and Les Miller, "Lightweight Agents for Intrusion Detection," Journal of Systems and Software, Elsevier, vol. 67, pp. 109- 122, 2003.

[11] R A Kemmerer, "NSTAT: a Model-based Real-time Network Intrusion Detection System", Technical Report TRCS97-18, Reliable Software Group, Department of Computer Science, University of California at Santa Barbara, 1997.

[12] A Mouinji, B L Charlier, D Zampunieris, N Habra, "Distributed Audit Trail Analysis", Proceedings of the ISOC 95 Symposium on Network and Distributed System Security", pp. 102-112, 1995.

[13] G Vigna, R A Kemmerer, "NetSTAT: A network-based intrusion detection system", Journal Computer Security, Vol. 7, No, 1, pp. 37-71, 1999.

[14] P A Porras, P G Neumann, "EMERALD: event monitoring enabling response to anomalous live disturbances", Proceedings 20th National Information Security Conference, NIST 1997.

[15] E. H. Spafford, D Zamboni, "Intrusion detection using autonomous agents", Computer Networks, 34, pp. 547-570, 2000.

[16] S Staniford -Chen, S Cheung, R Crawford, M Dilger, J Frank, J Hoagland, K Levitt, C Wee, R Yipi, D Z Erkle, "GriDS – a large scale intrusion detection system for large networks", Proceedings 19th National Information Security Conference, Vol. 1, pp. 361-370, 1996.