Effective Role of Mobile Agents based IPS (MAIPS) in Distributed Environment

R. Subalakshmi, M. Shiva Kumar, K. Krishnamoorthy

Abstract— As the need of IDS and IPS Technologies are increasing in this generation, in the same view point the concept of Agents activity is very important. Since the Mobility of Agents and their characteristics are profound, here in this paper the concept of IDS & IPS, with the act of Agents and their autonomous capability is expressed in the view of distributed Networks, hence this paper proposes a survey form based on the role of MA in IPS, wherein actual implementation is at par.

Index Terms— IDS, IPS, MA, HIPS, NIPS, MAIPS.

I. INTRODUCTION

Intrusion Detection Systems (IDSs) are proliferating throughout corporate, government, and academic computer networks. Because intrusion detection has become a mature industry and a proven technology, nearly all of the easy problems have been solved. No major breakthroughs in intrusion detection research have recently been made. Instead, commercial companies are mostly perfecting existing intrusion detection techniques. With the maturation of the intrusion detection field, traditional lines of intrusion detection research are having diminishing returns. Therefore, future intrusion detection research is expected to focus on relatively unexplored areas such as:

- ✓ Attack response mechanisms,
- ✓ Architectures for highly distributed intrusion detection systems,
- ✓ Intrusion detection inter-operability standards, and
- ✓ New paradigms for performing intrusion detection.

1.1 Intrusion Prevention System:

An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

The inadequacies inherent in current defenses has driven the development of a new breed of security products known as Intrusion Prevention Systems (IPS). This is a term which has provoked some controversy in the industry since some firewall and IDS vendors think it has been "hijacked" and used as a marketing term rather than as a description for any kind of new technology.

Whilst it is true that firewalls, routers, IDS devices and even AV gateways all have intrusion prevention technology included in some form, we believe that there are sufficient grounds to create a new market sector for true Intrusion Prevention Systems.

Manuscript received on July 2013.

Ms. R.Subalakshmi, Department of Information Technology, Kuppam Engineering college, kuppam, Chittoor Distrcit, Andhra Pradesh, , India.

Dr. M.Shiva Kumar,Department of information Technology,Sudharsan Engineering College, Pudukottai, Tamil Nadu, India.

Dr. K.Krishnamoorthy, Department of Computer Science and Engineering, Sudharsan Engineering College, Pudukottai, Tamil Nadu, India.

Within the IPS market place, there are two main categories of product: Host IPS and Network IPS.

✓ Host IPS (HIPS)

As with Host IDS systems, the Host IPS relies on agents installed directly on the system being protected. It binds closely with the operating system kernel and services, monitoring and intercepting system calls to the kernel or APIs in order to prevent attacks as well as log them. It may also monitor data streams and the environment specific to a particular application (file locations and Registry settings for a Web server, for example) in order to protect that application from generic attacks for which no "signature" yet exists.

One potential disadvantage with this approach is that, given the necessarily tight integration with the host operating system, future OS upgrades could cause problems.

Since a Host IPS agent intercepts all requests to the system it protects, it has certain prerequisites - it must be very reliable, must not negatively impact performance, and must not block legitimate traffic. Any HIPS that does not meet these minimum requirements should never be installed in a host, no matter how effectively it blocks attacks.

✓ Network IPS (NIPS)

The Network IPS combines features of a standard IDS, an IPS and a firewall, and is sometimes known as an In-line IDS or Gateway IDS (GIDS). The next -generation firewall - the deep inspection firewall - also exhibits a similar feature set, though we do not believe that the deep inspection firewall is ready for mainstream deployment just yet.

II. REQUIREMENTS FOR EFFECTIVE PREVENTION

In order to implement an IPS , One should concentrate on the requirements of the prevention policies in the networks, following lists certain requirements for effective prevention.

- ✓ In-line operation -
- ✓ Reliability and availability
- ✓ Resilience -
- ✓ Low latency
- ✓ High performance -
- ✓ Unquestionable detection accuracy -
- ✓ Fine-grained granularity and control –
- ✓ Advanced alert handling and forensic analysis capabilities.

III. MOBILE AGENT TECHNOLOGY

IDSs implemented using MAs is one of the new paradigms for intrusion detection. MAs are a particular type of software agent, having the capability to move from one host to another.

A software agent can be defined as [BRAD97]: "a software entity which functions continuously and autonomously in a particular environment … able to carry out activities in a flexible and intelligent manner that is responsive to changes in the environment … Ideally, an agent that functions continuously … would be able to learn from its experience. In addition, we expect an agent that inhabits an environment with other agents and processes to be able to communicate and cooperate with them, and perhaps move from place to place in doing so." Mobile agents have been a research topic of interest for several years, yet this research has for the most part remained within laboratories and has not experienced a wide-scale adoption by industry. The development of the World Wide Web application, however, has dramatically stimulated interest in this area of research by offering the possibility of a widely deployed application that could use mobile agent technology.

The research community visualizes mobile agents launched via web browsers to gather information and interact with any node in the network. IBM and General Magic were early pioneers of this vision, [CHES95, HARR95]. Concurrent with this effort, ARPA sponsored a Knowledge Sharing program. The KQML language [FINI94] was developed under this program and remains one of the viable Agent Communication Languages (ACLs). This research area was reformulated in the '95-'96 time frame when Java was released by Sun Microsystems. Although Java is simply a new interpreted computer language, it is designed for network interactions and is a powerful enabling technology for mobile code. Web browsers were quickly "Java-enabled" and the IT community seemed convinced that mobile code would quickly become a reality. The Java language provided some system independence and considerable security features were included in the language and implementations. These are not unique features, of course, they simply were implemented better in Java than other languages and so Java became extremely popular. During this same period, numerous proposals for mobile agent implementations were fielded. For example, the Lava system [WU96, HANS97] was developed at North Carolina State University. This system focused on security problems and developed a simple security policy for applets. Mitre Corporation [FARM96, FARM97] also pursued work in this area, developing authentication mechanisms and defining taxonomy of security related problems.

However, relatively little work has been done on using a mobile agent architecture for the purpose of providing a security capability, such as intrusion detection. If a mobile agent architecture is designed for a specific purpose such as system administration or security function maintenance, then strong authentication may be enforced and the residual risk decreases significantly. While MAs are an extraordinarily powerful tool, their implementation has been hindered by security considerations. These security considerations are especially critical for intrusion detection systems, with the result that most security research in this field has concentrated upon the architecture necessary to provide security for mobile agents. We claim that such negative results are not fatal to the proposed study since these security issues are likely to be addressed by the research community and there will be few authorized users of the MA-based IDSs within an organization.

3.1 Mobile Agents for Intrusion prevention systems

For mobile agents to be useful for intrusion prevention, it is necessary that many, if not all, hosts and network devices are installed with an MA platform. This is not a far-fetched assumption because an MA platform is general-purpose software that enables organizations to implement many different applications. If MAs become popular, every new host may come preinstalled with a MA platform just as today most personal computers come bundled with a Java interpreter in the web browser. Contrast this to many IPS schemes that assume that a host-based IPS is installed on every host. It is generally too expensive to install a proprietary solution (like a host-based IPS) on every host in a network, but it is not unusual to install a general-purpose interpreter (like an MA platform and Java virtual machine) on every host.

- Advantages

A number of advantages of using mobile code and mobile agent computing paradigms have been proposed [LANG98, SMIT88]. These advantages include:

- ✓ Overcoming Network Latency
- ✓ Reducing Network Load
- ✓ Asynchronous Execution and Autonomy
- ✓ Structure and Composition
- ✓ Adapting Dynamically
- ✓ Operating in Heterogeneous Environments
- ✓ Robust and Fault-tolerant Behavior
- ✓ Scalability

- Disadvantages

The obvious disadvantage of using MAs is the concern that they will introduce vulnerabilities into the network. However, this is not the only disadvantage to implementing Mobile Agent Intrusion Prevention System (MAIPS). MA solutions may not perform fast enough to meet the IPS's needs. In addition, the MAs may contain large amounts of code thus prohibiting rapid transfers between hosts. Finally, limited industry experience and modeling tools for formulating MA solutions to applications in general and IPSs in particular are also factors, as is the additional complexity involved in developing agent-based applications when compared with more traditional forms.

- ✓ Security
- ✓ Performance
- ✓ Code Size
- ✓ Lack of A Priori Knowledge
- ✓ Limited Exposure
- ✓ Coding and Deployment Difficulties

3.2 Useful Characteristics of MAs

MAs have many characteristics that enable them to enhance intrusion detection technology. Mobility is obviously one of the most important capabilities, and we can certainly benefit from it. However, other agent capabilities also lend themselves to intrusion detection technology. Agent technology and agent applications mimic collections of autonomous and intelligent individuals. This traditional distributed programming paradigm works well when components can be relied upon to function. Even by using redundant components, an attacker can disable a small finite number of backups.

This traditional design is easy to implement and is an efficient solution to many problems. Agent technology is a great contrast to this design since it attempts to give each agent an understanding of its environment along with the authority to independently make decisions.

- ✓ MAs are by nature autonomous, collaborative, self-organizing, and mobile.
- ✓ Picture a collection of MAs as a colony of bees.
- ✓ Another analogy is to picture a collection of MAs doing IPS work as a colony of ants.
- ✓ MAs can also be viewed as a collection of guards.

These are just a few examples of how colonies of autonomous mobile agents can benefit intrusion detection technology. Mobility is an important aspect, but that alone is not sufficient. MAs need to be able to operate autonomously and operate in consort with other agents. These features enable new intrusion detection paradigms.

IV. MULTI-AGENT IDS FRAMEWORK

The Specialized Local Agent is the engine component of our system. It must combine several kinds of attack analysis such as signature detection, anomaly detection and performed global analysis, for detecting distributed attacks. Due to the complex analysing tasks made by the SLA for detecting intrusions, the SLA delegates performed tasks to well defined agents and uses different data sources. As shown in figure 1, SLA delegates predetermined performed tasks to four agents (Filter, Analyser, Correlate, Interpreter and Mobile), and use two knowledge database (Event Rules, Events DB).

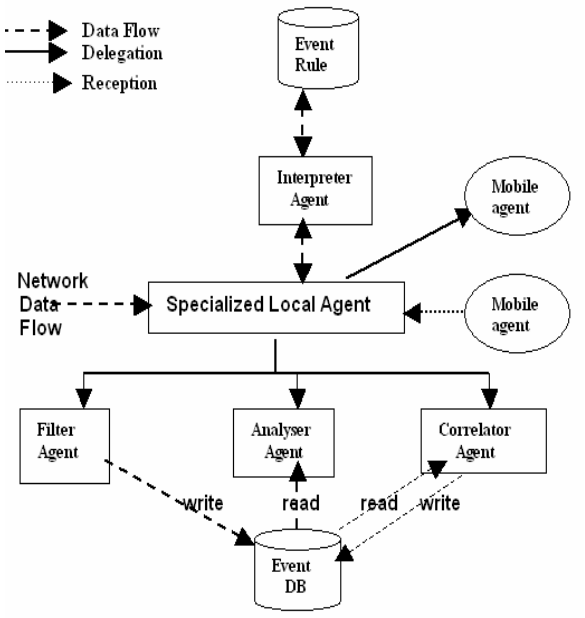

Figure 1. Multi-Agents Architecture

4.1 Effective Role of IPS with MA in Distributed Networks

As we are clear with the agents framework as shown in figure 1, the agents are replicated in-turn each agent is responsible for executing one task particularly, in deed the same concept of Mobile Agents Framework may be implemented in IPS too, As shown in Figure 2, the network which resembles an HOST Based IPS, s enabled with multiple network devices which are connected in network, wherein the agents wonder around the network in meeting the needs of IPS as discussed in Section **2**(Requirements for effective prevention), as per the architecture defined in figure 2, the agents like event agent, filter agent, analyzer agent, correlator agent, etc., together join hands in supporting the activity of IPS.

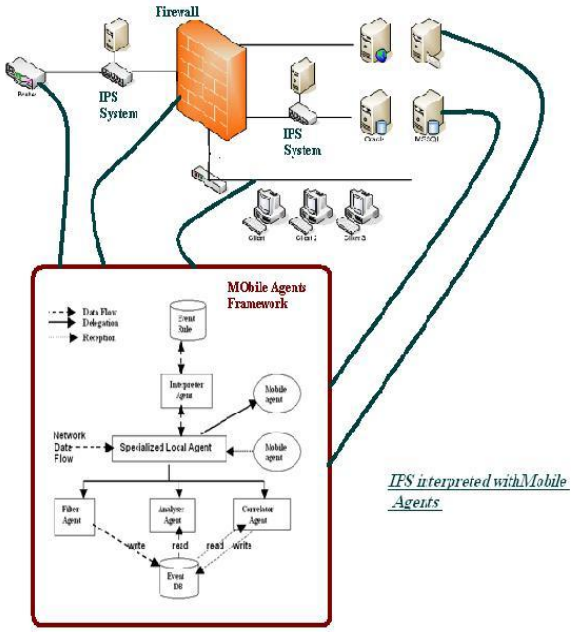

Figure 2. Architecture of IPS with Mobile Agents

V. CONCLUSION AND FUTURE WORK

The System I have proposed mainly concentrates on the advantages and role of MA in Host Based IPS, however keen concentration is required in considering the effects of prevention mechanism in HOST based IPS , further the concept of Either Anomaly or Signature based IDS need to be considered.

REFERENCES

1. Intrusion Prevention Systems (IPS) - January 2004, NSS Group.
2. M. Eid, “A New Mobile Agent-Based Intrusion detection System Using distributed Sensors”, In proceeding of FEASC, 2004.
3. G. Hulmer, J. S.K. Wong, V. Honavar, L. Miller, Y. Wang, “Lightweight Agents for Intrusion Detection”, Journal of Systems and Software 67 (03), pages 109-122, 2003.
4. M. Benattou and K. Tamine, “Mobile Agents Community For Distributed Intrusion Detection System”, accepted for publication in proceeding of International conference on Computing, Communication and Control Technologies, Austin, USA, July 2005.
5. C. Kruegel and T. Toth “Applying Mobile Agent Technology to Intrusion Detection”, technical report, University of Vienna, TUV-1841-2002-31, 2002.
6. Y. Zhang, W. Lee, and Y. A. Huang, 'Intrusion Detection Techniques for Mobile Wireless Networks', ACM J. Wireless Net., vol. 9, no. 5, Sept. 2003,
7. [BRAD97] Jeffrey M. Bradshaw, “An Introduction to Software Agents,” In Jeffrey M. Bradshaw, editor, Software Agents, chapter 1. AAAI Press/The MIT Press, 1997.
8. [CHES95] Chess, D., B. Grosof, C. Harrison, D. Levine, C. Parris, G. Tsudik, “Itinerant Agents for Mobile Computing,” IBM Research Report, RC 20010, March 1995. <URL: http://www.research.ibm.com/massdist>
9. [FINI94] Finin, T., R. Fritzson, D. McKay, and R. McEntire. “KQML as an Agent Communication Language,” Proceedings of the Third International Conference on Information and Knowledge Management (CIKM ’94), ACM Press, Nov. 1994.
10. [FRIN98] Frincke, D., Don Tobin, Jesse McConnell, Jamie Marconi, Dean Polla, “A Framework for Cooperative Intrusion Detection,” Proceedings of the 21st National Information Systems Security Conference, pp. 361-373, October 1998. <URL:

http://csrc.nist.gov/nissc/1998/papers.html>
11. [HANS97] Hansoty, Jatin N., "LAVA: Secure Delegation of Mobile Applets," Master's Thesis North Carolina State Univ., 1997. <URL: http://shang.csc.ncsu.edu:80/lava.html >
12. [HARR95] Harrison, C.G., D.M. Chess, A. Kershenbaum, "Mobile Agents: Are they a good idea?," IBM Research Report, March 1995.
13. [WHIT96] Gregory B. White, Eric A. Fisch, and Udo W. Pooch, "Cooperating Security Managers: A peer-based intrusion detection system," IEEE Network, 10(1), pp.20-23, January/February 1996.
14. [WU96] Wu, S.F., M. S. Davis, J. N. Hansoty, J. J. Yuill, S. Farthing, J. S. Webster, X. Hu. "LAVA: Secure Delegation of Mobile Applets," Technical Report 96/42, Center for Advanced Computing and Communication, North Carolina State Univ., Raleigh, NC, October 1996.
15. NIST Special Publication (SP) 800-61, Computer Security Incident Handling Guide, which is available at http://csrc.nist.gov/publications/nistpubs/.
16. GUIDE TO INTRUSION DETECTION AND PREVENTION (IDP) SYSTEMS (DRAFT) - Recommendations of the National Institute of Standards and Technology - Karen Kent & Peter Mell
17. [17]NIST SP 800-92 (DRAFT), Guide to Computer Security Log Management, which is available at.

AUTHORS PROFILE

Dr. M. Shiva Kumar, Professor, Department of IT, Sudharsan Engineering College, Pudukkottai, T.N, India.he has published papers in various conferences (National & international) He has good academic line of experience and published papers in various conferences (National & international)

Dr. K. KrishnaMoorthy, Professor, Department of CSE, Sudharsan Engineering College, Pudukkottai , T.N, India, has vast Experience and published papers in various conferences (National & international)

Ms.R.Subalakshmi,Currently Working has Associate Professor in the Department of IT, Kuppam Engineering College, Kuppam, having profound knowledge in research and area of interest is Network Security, Software Engineering, operating System Etc.,