Mobile agents in Intrusion Detection Systems: Advantages and Disadvantages

GEORGI TSOCHEV, ROUMEN TRIFONOV, OGNIAN NAKOV, SLAVCHO MANOLOV, GALYA PAVLOVA
Faculty Computer Systems and Technologies
Technical University of Sofia
Sofia, BULGARIA
gtsochev@tu-sofia.bg, r_trifonov@tu-sofia.bg, nakov@tu-sofia.bg, s_manolov@tu-sofia.bg, raicheva@tu-sofia.bg

Abstract: - Digitization of information in all spheres of human activity and use of technological innovations, as a basic case for the emergence of all wages and attacks that are insufficient to modern technologies and the continuous expansion of the complexity of security and hardware. The protection against these attacks and wages can be viewed in different directions in information and communication technologies. Computer security is defined as the protection of computer systems against threats to confidentiality, integrity and availability. Penetration is defined as a set of actions to compromise the integrity, confidentiality, and availability of resources. To monitor the events that occur in computer systems or networks is called intrusion detection system (IDS). This paper presents the mobile agent based technologies as a tool in IDS systems and their advantages and disadvantages.

Key-Words: - intrusion detection/prevention systems, agent based technologies, mobile agents, vulnerabilities

Received: October 13, 2019. Revised: April 1, 2020. Accepted: April 21, 2020. Published: April 27, 2020.

1 Introduction

Information security threats take many different forms. Some of the most common ones are software attacks, intellectual property theft, identity theft, device or information theft, sabotage, and manipulation of information. Most people have experienced some kind of software attack: viruses, worms, phishing and trojans are examples of such attacks. Intellectual property theft is a concern of many IT companies, with software theft being the most common. In the identity theft, the attacker tries to gain access to personal information in order to exploit it in a malicious manner. Device or information theft is common today because more and more information devices are mobile. Mobile phones are a common target of theft and are increasingly desirable as the volume of stored information increases. Sabotage can take the form of damaging a company's website in an attempt to harm consumers. The manipulation of information is intended to coerce the owner to pay for the restoration of the correct information or to recover his property.

Governments, the military, corporations, financial institutions, hospitals, and private companies accumulate a wealth of confidential information about their subjects, employees, customers, products, research, and financial transactions. Today, most of this information is collected, stored and processed by computers and transmitted over computer networks to other computers [17,19].

In the Department of Information Technologies in Industry, at the Faculty of Computer Systems and Technology, Faculty of Technical University Sofia, several years have been working on various research projects for finding the optimal solution in the automation of the process of penetration detection. Different scenarios have been developed linking different areas of artificial intelligence to IDS systems. Several applications have been developed to monitor the network behavior of various types of attacks and their proper detection. One of the main experiments was performed in the field of agent-based technologies, in particular stationary agents, and their combination with other types of AI methods. The results of the studies showed good levels of false positives and false negatives [9,10,11,12].

Implementing an effective way of detecting penetration is a high goal that is not easily solved or by a single mechanism. This development will look at different ways in which mobile agents can be applied to the problem of intrusion detection and response. Not only the benefits of mobility but also those of software agents in general will be addressed.

Research into this area has outlined a number of ways to deploy mobile agent technology to address the shortcomings of current IDS designs and implementations and related security issues. Several new approaches are also considered to respond automatically to a failed penetration attempt. The purpose of this article is to introduce the use of mobile agents as a tool for new types of information security solutions, to show their advantages and disadvantages in this field of intrusion detection prevention systems.

2 Security objectives in IDS

2.1 Some Intrusion detection systems

2.1.1 SNORT

Intrusion detection and prevention systems are widespread nowadays based on the huge number of network security attacks. One of the most well-known and powerful systems in the field of network security management is Snort. It is a free and open source system created by Martin Roesch in 1998, developed and operated by Sourcefire. Later in 2013, the company sold all Snort rights to Cisco, which to this day has been developing and developing this system.

Snort is known for having the ability in real time to perform traffic analysis and log TCP / IP network packets in a log file. Traffic analysis focuses on protocol analysis, search and content matching. In addition, Snort can also be used to detect attacks aimed at trying to disrupt the fingerprint system, buffer overflow, scanning network ports, etc.

2.1.2. Cisco

Cisco provides an extensive set of security features in their different security products, such as Defeat Distributed Denial-of-Service Attacks, Cisco Intrusion Prevention System (IPS) sensors, and etc. However, common for all solutions and products is that Cisco is still using common security solutions to protect networks. Those security solutions fail to provide adequate level of protection, because of ever increasing security incidents. The main reason is still using the traditional signature–based approach for many products [18].

2.1.3 Nessus™

Nessus is a vulnerability scanner that provides couple of good features like efficient discovery of vulnerabilities, network configuration and auditing, asset profiling etc. However, the major problem with Nessus is that it requires significant involvement of security administrators [18].

2.2 Disadvantages of ordinary IDS

An intrusion detection system (abbreviated IDS) is a security system that detects hostile activity on the network [1]. The key is to detect and possibly prevent actions that could compromise the security of the system or attempt to interrupt the operation, including exploration / data collection phases, which include, for example, port scanning. One of the key features of intrusion detection systems is their ability to provide an overview of unusual activity and to issue alarms, notify administrators and / or block suspects' connections.

Modern IDSs are not perfect. Developers continue to address the shortcomings by improving and refining existing techniques, but some shortcomings are inherent in the way IDS is built. The most common disadvantages include the following elements [4,5,6,7]:

- High Fake Alerts: Most IDSs detect system-wide attacks by analyzing information from a single host, single application, or single network interface across multiple locations across the network. There are many false alarms and the detection of attacks is not perfect. Lowering the thresholds for reducing false alarms increases the number of attacks that go through undetected as false negatives. Improving the ability of IDS to accurately detect attacks is a major problem facing IDs.
- Difficult maintenance: Configuring and maintaining intrusion detection systems often requires specialized knowledge and considerable effort. For example, malpractice detection is typically accomplished by using an expert system wrapper that encodes and matches signatures using rule sets. The set of upgrade rules includes details specific to the expert system and its language for expressing rules, and can only allow an indirect clarification of the consistent relationships between events. Similar considerations may also apply to the addition of a statistic commonly used to detect unusual behavioral abnormalities.
- Limited Flexibility: Intrusion detection systems are typically written for a specific environment and have proven difficult to use in other environments that may have similar policies and problems. The detection

mechanism can also be difficult to adapt to different usage patterns. Having system-specific detection mechanisms and replacing them over time with improved detection techniques is also a problem with many IDS implementations. Often IDS needs to be completely restarted to make changes and additions.

- Direct Attack Vulnerability: Due to dependency on hierarchical component structures, many IDSs are vulnerable to attack. An attacker can break an IDS control branch by attacking an internal node or even "decapitate" the entire IDS by removing a command and control node at the root. Typically, such critical components are found on platforms that cannot resist a direct attack. However, the current implementations lack other techniques to deal with the issue such as redundancy, mobility, dynamic recovery, etc.
- Fraud vulnerability: Network IDS evaluates network packets using a common network protocol stack to model the behavior of the host protocol stack it protects. Attackers take advantage of this mismatch by sending specially adapted packets to the target host, which are interpreted differently by IDS and the target. This can be done in various ways, such as changing fragmentation, sequence numbers and banners [6]. The attacker penetrates the target while the IDS is either "blind" to the attack, or is misled to interpret the target as opposing the attack.
- Limited response capacity: IDS has traditionally focused on detecting attacks. While the discovery serves a useful purpose, the system administrator is often unable to immediately analyze IDS reports and take appropriate action. This gives the attacker a window in which to act freely before being counteracted by the administrator's actions. Many IDSs are beginning to deploy auto-responding capabilities to significantly reduce the time available for attackers to expand their reach into the network. However, they are limited in their ability to adapt dynamically to attack.
- No generic methodology: Overall, the costs of building IDS from the components available are significant, largely due to the lack of a structured methodology. No such structuring insights emerge from the field itself. This may be due in part to a lack of agreement on intrusion detection techniques.

In addition to these drawbacks, IDS is constantly faced with new obstacles that must be overcome. Some recent obstacles include the following issues [3]:

- End-to-end encryption: With enhancements to the security of communications protocols, end-to-end traffic encryption capabilities are increasing.
- High-speed communications: Higher communication speeds have a direct effect on the processing speed needed to analyze the contents of a packet, which can lead to lost packets. The trend towards switched communication by broadcasting also increases the difficulty for network IDS to monitor multiple communication flows.
- Attack Width: As new attacks are created, IDS must be updated to detect them. While new attacks are often added, old ones can rarely be removed. Usually, the larger the attack coverage, the more processing time is required by the detection algorithm.
- Technological limitations: It is not possible to create a security program to detect the presence or absence of malicious codes within arbitrary programs or protocols. As existing services evolve and new services are introduced, intrusion detection techniques are faced with the prospect of reducing returns - greater investment is needed in time for less efficiency gains.

3. Mobile agents

A software agent is a program that can empower an individual unit or an entire organization, work independently to achieve a goal, meet and interact with other agents and their environment. The software agent contains the code and status information required to perform some computations and requires the agent's platform to provide the computing environment in which it operates. Agents can be static or mobile. Landline agents remain on one platform while mobile agents are able to stop processing on one platform and move to another platform where they continue to execute their code. Mobile software agents provide a new and useful paradigm for distributed computing. Unlike the client-server computing paradigm, the relationships between entities are more dynamic and mutually reinforcing, emphasizing autonomous collaboration.

Figure 1 depicts the movement of an agent between several agent platforms. The platform from which the agent originates is called the initial platform and is usually the most reliable agent environment[4]. One or more hosts may include an agent platform, and the agent platform may support multiple or meeting venues where agents can interact.

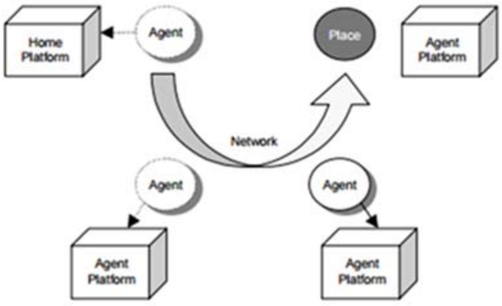

Fig. 1 Overview of mobile agents

Mobile Agent Technology takes advantage of the work done on intelligent agents that focuses on static autonomous agents capable of applying application domain knowledge, as well as developing software systems capable of supporting mobile code on heterogeneous hardware technologies (such as Java technology). Intelligent agents embody the ability to decompose and solve problems together. Agents observe their environment, cause of action, and other agents, interact with other agents, and perform their actions simultaneously with other agents. Interactions can convey facts or beliefs through an agent's communication language and can depend on the ontology to gain a common understanding of the situation. A significant number of mobile agent systems have been developed at universities and in the industry. Although mobile agents retain the characteristics of autonomy and collaboration, as with smart agents, the focus is on mobility features, which often rely on simple, easy algorithms for reasoning and collaboration through a less sophisticated interpretation of messages.

There is considerable debate about the benefits of deploying mobile agent systems instead of client-server, transaction processing and other well-established technologies. This debate continues today. Ultimately, such decisions must be made about the specifics of the application and the appropriateness of the engineering solution technology. It is believed that penetration detection and response is an area of application suitable for software agents. In particular, the ability to move computation between different nodes offers advantages over IDS that rely on statically spaced calculations.

In order for mobile intrusion detection agents to be deployed, participating nodes (ie hosts and network devices) must have an agent platform installed. Because many agent systems work on a wide variety of hardware and software, this requirement is not as difficult to meet as it may appear[8]. With the help of mobile agent technology, assembly nodes, internal aggregation nodes, and commands and control nodes need not be permanently on the same physical machine. For example, a mobile agent can function as an aggregation node and move to any physical location on the network that is best suited for its purposes. The mobile agent paradigm also offers specialization - agents can be different for different functions, each looking for separate attacks and processing data accordingly.

Mobile agent technology can potentially overcome a number of limitations inherent in existing IDS that use only static components. For example, mobility and autonomy make them ideal for detection schemes that follow "cop on the beat", "immune system" or other real analogy. This does not mean that the characteristics of mobile agents are sufficient in themselves to achieve improvements in IDS. When deploying mobile agents to this application domain, careful design decisions are still needed to take advantage of their features [5]. In particular, the type of knowledge level coordination required to detect and respond to invasions places many requirements on agents, including locating other agents with the necessary capabilities, communicating effectively with them through a common mutually intelligible vocabulary, and coordinating actions that should to jointly address a situation.

A number of advantages of using paradigms for calculating mobile codes and mobile agents over their static counterparties have been identified in the past [2] and are relevant to intrusion detection systems.

- Overcome network delays: Mobile agents can be deployed to perform operations directly at a remote point of interest, allowing them to respond in real time to changes in their environment. In addition to detecting and diagnosing potential network intrusions, mobile agents can provide appropriate response mechanisms. Such actions include gathering information about an attack sent or broadcast by the target of an attack, closing or isolating a system under attack to protect it from further damage, tracing the path of attack, and closing or isolating the attacker's system if the attack is launched by an internal host;

- Reducing network load: Instead of transferring data to the network, mobile agents can be sent to the machine on which the data resides, while moving the calculation to the data instead of transferring the data to the calculation, thereby reducing network load. A side benefit of privacy concerns is the efficiency of moving an encrypted agent and its precision data, compared to moving all raw data in encrypted form;
- Autonomous and asynchronous implementation: For large distributed systems, the ability of the system to continue to operate when parts of it are destroyed or isolated is essential. Mobile agents can exist and function independently of the emerging platform, making them useful as IDS components, since attack surviving agents can reconstruct damaged components (eg by cloning) and restore their functionality;
- Dynamic adaptation: The ability of mobile agent systems to recognize the environment and respond to change is useful in detecting penetration. Agents can move elsewhere to gain a better position or avoid danger, clone for redundancies and concurrency, or order other assistants. Agents can adapt to favorable and unfavorable situations. When combined with standalone and asynchronous execution, these features make it easy to build robust and fault-tolerant systems;
- Platform Independence: Agent systems provide an abstract computing environment for agents, regardless of the hardware and software of the computer on which they run. These features make it an appropriate wide-ranging environment for network management applications in general and intrusion detection in particular, which allows the relative free movement of agents in a given area. This is especially useful for response mechanisms, because when intrusion is detected, remedies can be applied or initiated from almost anywhere on the network. Likewise, discovery mechanisms also benefit from widespread mobility with the potential to easily collect and merge data from different network sources;
- Protocol encapsulation: In conventional systems, the host has an interface between the communication units, requiring any changes to be synchronized for continuous interaction. Mobile agents can directly include the protocol and lead to an upgrade of the interface with the movement of an agent to another host;
- In addition to these advantages, mobile agents allow a natural way to structure and design IDS. Agent orientation and mobility considerations provide an effective maximum for data organization and functionality. Agents are inherently prone to designs that have the desired high adhesion and low-modulus properties.

Although it is of interest to apply mobile agents to penetration detection, full mobility of all components is unlikely to be effective in practice because of the associated overhead. Therefore, some IDS components are either designated as static agents or remain static after they are deployed [7]. This allows the mobile agent paradigm to be applied, but is only based on mobility where appropriate. Other practical factors, such as trust relationships, performance capabilities, and physical location, can also limit mobile agents to a subset of available agent platforms.

4 Mobile agents in IDS

Although mobile agents do not directly improve detection techniques, they can reformulate the way techniques are applied, thereby improving efficiency. One potential area of use is reducing the huge amount of distributed log data moved between internal nodes in the conventional IDS hierarchy. Having agents who visit data warehouses and monitoring results is an ideal alternative that is appropriate for mobile agents' ability to transfer calculations to data. In addition to reducing network load, the approach causes specialized agents to focus on specific classes of intrusion, such as coordinated attacks, which occur over long periods of time from different sources.

Another area of use is to minimize the ability of a hacker to mislead IDS by mismatches between the IDS protocol model and the target protocol stack. Because agents can replicate and reside on different platforms, they can potentially eliminate such conversations. Switching from network IDS to multiple host-based discovery agents running concurrently also reduces the possibility of incident packets occurring, maximizing the potential for triggering a rapid response to an open intrusion system. In addition, deploying other components on the host provides the only IDS tool to see the packets in clear text in situations where the host uses network-level encryption (eg Internet Protocol Security (IPSec)).

Mobile agents can facilitate the deployment of robust, attacking IDS architectures [2]. Agents can move around in capturing danger or suspicious activity, clone for reservation or replacement, work autonomously and asynchronously from where they were created, collaborate and share knowledge and self-organize (e.g., dynamically reconfigure relationships, to offset the failure of key components). In addition, agents are susceptible to genetic diversity, which also helps to avoid attacks aimed at circumventing known and stable IDS detection mechanisms[16].

- The greatest potential for mobile agents is a response rather than a discovery. Because reactions can be initiated from almost anywhere on the network, mobile agents can handle attacks in a more optimal way than in conventional IDSs. Mobile agents improve IDS's ability to track an attacker through an attacked network, respond to a target, respond to a source, collect evidence of attack from a host and network components, and isolate the source and target. The following elements describe some of the benefits of using mobile penetration agents[13,14]:
- Attacker Tracking: Attackers often enter a chain of multiple hosts before attacking a target and sometimes missing their exit address. To find the attacker, IDS must follow the chain and find the real host that starts the packets. To make such a mark, IDS needs the ability to suppress each Ethernet segment and analyze each host. Typically, the infrastructure needed would be too expensive, but not with a widely installed agent platform;
- Answer the target: When an attack is detected, it is vital to respond automatically to the target host. A quick response can prevent an attacker from creating a better position and using a penetrated host to compromise the network. It can also minimize the effort required to repair the damage done by the attacker;
- Source Response: The attacker's host response gives the IDS much more power to limit the attacker's actions. Without the use of mobile agents, IDS is unlikely to have sufficient access to the attacker's host to take corrective action. While this option has limitations, since it requires an agent platform to be active on the attacker's host and the attack to come from the management domain, it also has the potential to be a very effective part of the IDS arsenal[15];
- Evidence gathering: It is currently impossible to automatically gather evidence of attack from many different sources. The problem is you have the right software running at the right place at the right time. Mobile agents offer the ability to work anytime, anywhere at any time, making it possible to present evidence from different hardware platforms, different operating systems, and even different applications such as web servers. Mobile agents can also intelligently audit the network by dynamically reconfiguring the audit capabilities of their respective hosts for strong auditing of suspicious or important network locations[14];
- Source and Target Isolation: Since auto-target and source response actions may fail, a network-level response is ultimately required to limit the attacker's actions. There are three common strategies: block target communications, block attacker communications, and block target-attacker communications. The ability of mobile agents to travel to all network elements to take corrective action is what enables them to execute these strategies[13,14,15].

Table 1 Advantages and Disadvantages of M-agents

Advantages	Disadvantages
Mobile agents add error tolerance. The network is not vulnerable to a single failure point.	Mobile agent tools can have bugs and security vulnerabilities that are still unknown.
It is more difficult for an intruder to disable security tests and monitors when they are distributed over the network.	Network test packages are relatively large. Manage very light agents introduces additional communicate and control costs.
Mobile agents can take advantage of the inherent parallelism of large networks to offer performance improvements over traditional centralized security monitoring by distributing the load of network security tests.	Mobile agents are not mature technology and most agent development tools are in alpha or beta versions.
Distributed security testing scales and more agents can be added when new computers are added to the network. Maintaining and upgrading a security test kit can be accomplished by sending or cloning new agents and harvesting or disposing of old agents.	Although an agent's ability to navigate the network introduces fault-tolerant security features, it also exposes agents to new security threats and risks that host-based security tools do not encounter.
Agents can be tailored to a variety of tasks, spanning a range of responsibilities from penetration detection and diagnostics to reconfiguration and	The agent environment must be installed and maintained at each node.

recovery.	
Agents can be designed to work with heterogeneous computer systems and take advantage of the embedded agent's communication capabilities.	

5 Conclusion

Agents seem to be a very useful approach when building a large set of network applications. Therefore, a secure way to use agents is essential to making them viable on public networks, such as the Internet.

The purpose of this article was to introduce the use of mobile agents as a tool for new types of information security solutions. The idea is to offer flexible and effective solutions to a problem that is difficult to handle with conventional approaches.

The distributed nature of mobile agents makes it harder to bypass or disable security tests than with a central monitor or host-based security check approach. The lightweight design of the agents themselves allows them to be easily updated or dropped when new vulnerabilities are discovered or old vulnerabilities are addressed. Mobile agents are suitable for network management applications in a heterogeneous environment. A browser plug-in agent would help network administrators put systems to use more easily. The encryption of agents and their messages and the use of digital signatures provide some security measures, but further research is needed on the security of agents, their context and their protocols.

ACKNOWLEDGMENTS

This research is realized under the national science program “Information and Communication Technologies for common digital market in science, education and security” managed by Ministry of Education and Science.

References:

[1] Трифонов, Р. ЛЕКЦИИ ПО ДИСЦИПЛИНАТА “СИСТЕМИ ЗА СИГУРНОСТ”

[2] Wayne A. Jansen, INTRUSION DETECTION WITH MOBILE AGENTS

[3] Jai Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, E. H. Spafford, and Diego Zamboni, “An Architecture for Intrusion Detection using Autonomous Agents,” Department of Computer Sciences, Purdue University; Coast TR 98-05, 1998.

[4] Karima Boudaoud, Houda Labiod, “MA-NID: A Multi-Agent System for Network Intrusion Detection,” Eighth International Conference on Intelligent Systems, June 1999.

[5] Giacomo Cabri, Letizia Leonardi, Franco Zambonelli, “The Impact of the Coordination Model in the Design of Mobile Agent Applications,” Twenty-second Computer Software and Applications Conference (COMPSAC), August 1998.

[6] S. Staniford-Chen, et al., “GrIDS – A Graph Based Intrusion Detection System for Large Networks,” Nineteenth National Computer Security Conference, pp.361-370, October 1996.

[7] David Chess, Benjamin Grosof, Colin Harrison, David Levine, Colin Parris, Gene Tsudik, “Itinerant Agents for Mobile Computing,” IEEE Personal Communications, 2(5), pp.34-49, October 1995.

[8] Michael Conner, Chirag Patel, and Mike Little, “Genetic Algorithm/Artificial Life Evolution of Security Vulnerability Agents,” Army Research Laboratory Federal Laboratory Third Annual Symposium on Advanced Telecommunications & Information Distribution Research Program (ATIRP), February 1999.

[9] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, G. Pavlova. Increasing the level of network and information security using artificial intelligence. Fifth Intl. Conf. Advances in Computing, Communication and Information Technology- CCIT 2017, 2017, E-ISBN:978-1-63248-131-3, DOI : 10.15224/978-1-63248-131-3-25, pp. 83 - 88

[10] R. Trifonov, R. Yoshinov, G. Pavlova, G. Tsochev. Artificial neural network intelligent method for prediction. Mathematical Methods and Computational Techniques in Science and Engineering, AIP Conf. Proc. Vol. 1872, doi: 10.1063/1.49966781872, Cambridge, UK, 2017, ISBN:978-0-7354-1552-2, pp. 020021-1 - 020021-6 (SJR = 0.163)

[11] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, G. Pavlova. A Survey of Artificial Intelligence for Enhancing the Information Security. International Journal of Development Research, Vol. 07, Issue, 11, November, 2017, ISSN:2230-9926, (SJIF: 5.667) , pp.16866-16872

[12] R. Trifonov, G. Tsochev, S. Manolov, R. Yoshinov, G. Pavlova. Conceptual model for

cyber intelligence network security system. International Journal of Computers, Volume 11, 2017, ISSN: 1998-4308, pp. 85-92

[13] Agent-Based Model of Computer Network Security, Vladimir I. Gorodetski, O. Karsayev, A. Khabalov, I. Kotenko, Leonard J. Popyack and Victor Skormin

[14] Mobile agents and security, W. A. Jansen

[15] Security Issues in Agent Based Computing, Michel Abdalla, Walfredo Cirne, Leslie Franklin, Abdallah Tabbara

[16] Selected Security Aspects of Agent-based Computing, Piotr Szpryngier, Mariusz Matuszek

[17] Checharova, N., K. Chehlarova, Verification and Improvement of Digital Competence and Common Culture through Symmetries, In: Electronic Collection of “Instruments for Attractive Education” with ISBN 978-619-90168-4-8

[18] Shibli, Awais & Muftic, Sead. (2008). Intrusion Detection and Prevention System using Secure Mobile Agents.. 107-113.

[19] G. Popov and K. Raynova, "Diversity in nature and technology — Tool for increase the reliability of systems," 2017 15th International Conference on Electrical Machines, Drives and Power Systems (ELMA), Sofia, 2017