A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems

Saidat Adebukola Onashoga, Adebayo D. Akinde, and Adesina Simon Sodiya
Department of Computer Science, University of Agriculture, Abeokuta, Nigeria

bookyy2k@yahoo.com; sinaronke@yahoo.co.uk; ada2@charms.org

Abstract

Intrusion Detection Systems (IDS) is defined as a component that analyses system and user operations in computer and network systems in search of activities considered undesirable from security perspectives. Applying mobile agent (MA) to intrusion detection design is a recent development and it is aimed at effective intrusion detection in distributed environment. From the literature, it is clear that most MA-based IDS that are available are not quite effective because their time to detection is high and detect limited intrusions.This paper proposes a way of classifying a typical IDS and then strategically reviews the existing mobile agent-based IDSs focusing on each of the categories of the classification, for example architecture, mode of data collection, the techniques for analysis, and the security of these intelligent codes. Their strengths and problems are stated wherever applicable. Furthermore, suggested ways of improving on current MA-IDS designs are presented in order to achieve an efficient mobile agent-based IDS for future security of distributed network.

Keywords: IDS, Mobile Agents, Data Mining

Introduction

An intrusion is defined as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. An intrusion takes place when an attacker or group of attackers exploit security vulnerabilities and thus violate the CIA guarantees of a system. Intrusion detection is therefore required as an additional wall for protecting systems. Intrusion detection is simply an act of detecting intrusions.

Intrusion Detection System (IDS) is an authorized way of identifying illegitimate users, attacks and vulnerabilities that could affect the proper functioning of computer systems. IDSs detect some set of intrusions and execute some predetermined actions when an intrusion is detected (W. Wang et al., 2006). However, the initial designs of IDS are faced with some shortcomings listed as follows:

(i) Delay of time.
(ii) A single point of failure.
(iii) Limited scalability.
(iv) Hard to communicate mutually between different IDSs

In order to solve the aforementioned shortcomings, mobile agent technology is currently applied to IDS. Mobile agent is a particular type of software agents which has the capability of moving from one host to another. It is an autonomous program situated within an environment, which senses the environment and acts upon it using its knowledge base to achieve its goals. Mobile agent is of the features of reducing network overload, overcoming network latency, synchronous and autonomous execution, robustness and fault-tolerance, system scalability and operating in heterogeneous environments. To this end, MA technology is very suitable to solve intrusion detection in a distributed environment (Chan & Wei, 2002), hence the advent of Mobile Agent-based IDS (MA-IDS).

MA-IDSs are also faced with some shortcomings such as:

a. *High time to detection:* MA solutions may not be fast enough to meet the needs of IDS. One of the major challenging problems facing MA-IDS is improving the speed with which they can identify malicious activities.

b. *Performance:* though MA technology has improved greatly on detection performance, but effective detection of autonomous attacks is still very low. Also, agents are often written in scripting or interpreted languages, which are easily ported between different platforms. Their mode of execution is still very low compared to native codes (Kruegel and Toth, 2002).

c. *Security:* Another major problem is protecting the protector (MA-IDS) from attacks.

Hence, the thrust of this paper is to critically examine the existing and most referenced MA-IDSs. The paper is organized as follows: the second section discusses the proposed classification of Intrusion detection system; the third section examines the existing literature on MA-IDSs; in the fourth section, the proposed architecture is discussed considering the shortcomings of current design; the fifth section concludes the work.

Classification of Intrusion Detection System

It is a well-known fact that the research in a field greatly benefits from a good taxonomy and hence a good classification. There have been several defined taxonomies, classifications and subsequent surveys for intrusion detection. The goals of the efforts in several classifications have also been quite diverse; some only try to survey the field and find it easier with labels on the systems, while others try to use the taxonomies for a deeper understanding or to guide future research efforts.

Despite these previous efforts, intrusion detection still lacks a widely applicable and accepted taxonomy. This may in part be because of it being a young research field, part of it being fast-paced and maybe part of it owing to its inherent complexity (Almgren et al., 2003). This paper aims to broadly classify IDS based on its necessary features. Figure 1 shows our proposed classification of a typical intrusion detection system and its description follows.

Each of these classifications is described below:

Architecture

In a hierarchical architecture, the leaf nodes represent network-based or host-based collection points at which information is gathered. The event information is passed to internal nodes, which aggregate information from multiple leaf nodes. Further aggregation, abstraction and data reduction occur at higher internal nodes until the root node is reached. The root node is a command and control system that is responsible for detecting intrusions and for issuing responses. A network IDS architecture allows information to flow from any node to any other node. The data collection,

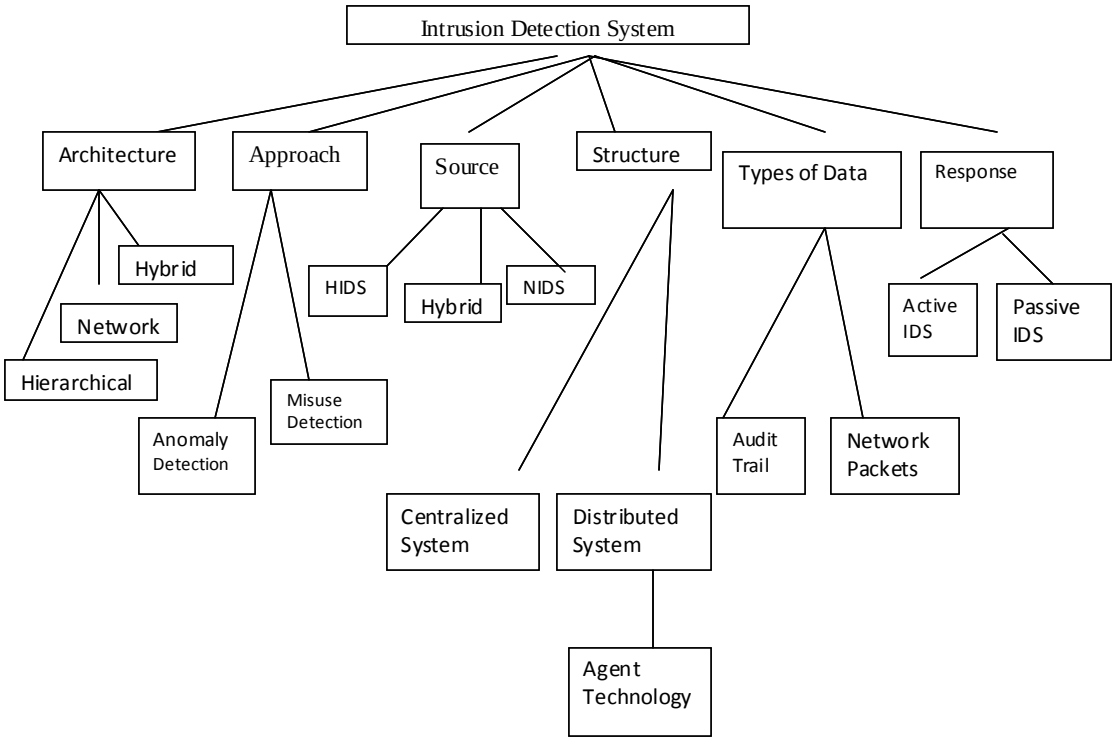

Figure 1: Classification of IDS

aggregation, as well as the command and control functions are consolidated into a single component located on every monitored system while a Hybrid IDS architecture is a combination of both hierarchical and network IDS architectures.

Intrusion Detection Approach

Intrusion detection is classified into two types: misuse and anomaly detection. Misuse intrusion detection uses well-defined patterns of the attack that exploit weaknesses in system and application software to identify the intrusion. These patterns are encoded in advance and used to match against the user behaviour to detect intrusion. Anomaly intrusion detection uses the normal usage behaviour patterns to identify the intrusion. The behaviour of the user is observed and any deviation from the constructed normal behaviour is detected as intrusion (Kazienko & Dorosz, 2004).

Source

When considering the area being the source of data used for intrusion detection, another classification of intrusion detection system can be used in terms of the type of the protected system. There is a family of IDS tools that use information derived from a single host system – host based IDS (HIDS) and those IDSs that exploit information obtained from a whole segment of a local network – network based IDS (NIDS). A Hybrid IDS exploits information from both HIDS and NIDS

Structure

Since the concept of IDS was introduced in 1980 (Anderson, 1980), many IDSs have been designed and implemented for centralized systems. In the centralized IDS, data analysis is performed in a fixed number of locations, independent of how many hosts are being monitored.

In a distributed system, IDSs must analyze large volumes of data while not placing a significant added load on the monitored systems and networks. Data must be obtained from sources distributed around the computing system. This introduces the agent technology, where mobile agents are distributed across the network gathering information intelligently and autonomously. Mobile agent based- IDS overcome the shortcomings of the centralized system by exploiting the mobility paradigm of the agents to perform distributed correlation.

Types of Data

Every project on developing or testing intrusion detection systems uses some kind of data. Many papers do not really focus on data collection but reveal a great deal of information about the data sources they used (Sodiya, 2004). The types of data gathered from different sources include:

- Audit Trails are logs of events in a network environment.
- Network Packets are units of information transmitted form one computer to another in a network environment.

Response

Response mechanism can also be classified into passive and active (Base and Mell, 2002) according to whether they rely on third parties to be carried out. In that sense, notifying an administrator would be considered as a passive response, while blocking network traffic through a firewall would be active.

Current MA-IDSs

Mobile agents have been proposed as a technology for intrusion detection applications. Rationale for considering agents in an IDS ranges from increased adaptability for new threats to reduced communication costs. Since agents are independently executing entities, there is the potential that new detection capabilities can be added without completely halting, rebuilding and restarting the IDS.

The following is the research that has been done in the area of MA-IDS, focusing on architecture, mode of data collection, security and their strengths and weaknesses.

DSCIDS - Distributed Soft Computing for Intrusion Detection System by Abraham et al. (2007)

Architecture

The paper is based on a hierarchical architecture with Central Analyzer and Controller (CAC) as the heart and soul of the DIDS. The CAC usually consists of a database and webserver which allows interactive querying by the network administrator for attack information/analysis and initiate precautionary measures. CAC also performs attack aggregation, building statistics, identify attack patterns and perform rudimentary incident analysis.

Data Collection

The mode of data collection is not discussed but the algorithm is tested on the KDD cup 1999 dataset whose source is network based.

Techniques

The authors tested the model using different soft computing techniques which consists of neural network, fuzzy inference system, approximate reasoning and derivative free optimization techniques on a KDD cup dataset. The experiments have three phases namely: input feature reduction, training phase and testing phase. In the data reduction phase, important variables for real-time intrusion detection are selected by feature selection. In the training phase, the different soft computing models are constructed using the training data. The test data is then passed through the saved trained model to detect intrusions in the testing phase.

Strengths

The problem faced with hierarchical architecture is being solved by allowing a free communication between the layers. A well comparative analysis of the different soft computing algorithms with other machine learning techniques, is being carried out which serves as references for researchers in the field

Problems

The agents are not well distributed. The full description of how the agents detect intrusions based on the soft computing algorithms proposed is not well discussed.

MSAIDS – Multi-Level and Secured Agent-based Intrusion Detection System by Sodiya (2006)

Sodiya (2006) focused on (i) improving IDS performance
(ii) detection of autonomous attack using its architecture
(iii) Reduction in false alarm
(iv) IDS agents security

Architecture

The architecture provides a methodology where intrusion is done at two levels. The first is the Lower Level Detection (LLD), which has the data agents and processing agents. The data agents move around the nodes in the network to collect associated information. The 2 processing agents also known as node agents where Node-1 agent is responsible for construction of the first level database from the information collected and for data cleansing, classification and formatting. The Node-2 agent is responsible for data mining and first level intrusion detection and communicates the possibility of intrusions to the interface agent through the alarm agent.

The Upper Level Detection (ULD) also known as confirmation level is involved in separate intrusion detection process. At the ULD, the lower level agents gather data from the data agents and inform the Controller and Protector (CP), which acts as the Facilitator agent about the nature of the data gathered. The CP also ensures proper communication and delivery of service among agents. The data gathered are then used to update the ULD database; the ULD does not check for intrusion if there is no signal from the LLD.

Data Collection

The types of data collected are application messages, authentication events, system calls, TCP connections.

Techniques

An Apriori algorithm is modified to extract patterns by the first level and second level agents.

Security

MSAIDS maintains security of agents by using asymmetric cryptosystem of the Aglet's framework. In addition to this, agents' states are recorded and authenticated before they are initiated.

Response

Any suspected intrusion is reported by the Interface Agent to the Site Security Officer (SSO). The action to be taken by the SSO is not stated.

Strengths

In addition to securing mobile agents, the use of recorded state mechanism, which has been proved effective, is a plus in this work. The agents are well coordinated.

Problem

1. The activities at the ULD could still be integrated with the LLD to form one-level architecture and have the CP at the ULD since detection of intrusion at each level is still based on same algorithm. It took 0.14 seconds to report an intrusion at the LLD and 0.75 seconds at the ULD.

2. The architecture presented does not provide adequate security for the database, which could be vulnerable to changes by attackers.

Mobile Agent for Network Intrusion Resistance by H. Q. Wang et al. (2006)

Architecture

The designed system framework includes the following components:

(i) Manager: the centre of controlling and adjusting other components and it maintains their configuration information. The manager receives intrusion alarms from host monitor MA and executes intrusion responses using intrusion response MA.

(ii) Host monitor MA: this is established on every host in the network. If intrusions occur confirmatively, the host monitor MA will appeal to the manager and report the suspicious activity directly. After receiving the appeal, the manager distributes a data gathering MA patrolling other hosts in the network to gather information. If a distributed intrusion is found, the manager will assign an intrusion response MA to respond intelligently to every monitored host. The database of configuration stores the node configuration of detecting system.

Data Collection

The data source of IDS is both host-based and network-based. The gathering part of data source is to record, filter and format the connection information of the monitored host and write them into the log. The types of data collected includes system log and some conserved audit records.

Techniques

The intrusion analysis MA mainly analyses the log file in the monitored host system and compares them with the characters of known attack activities to find abnormal activity combined with different detection measures which were not mentioned.

Security

The framework's security is based on the security measures provided by Aglet

Response

The intrusion response MA responds to the intrusion events that occur which can include tracking the intrusion trace to find the intrusion fountain, recording the intrusion events into database etc.

Strengths

It changes the hierarchical system structure of traditional distributed IDS.

Problem

There is a control center carrying out the major part of the intrusion detection, if the location of this center is discovered, then the system collapses.

An Adaptive Intrusion Detection and Defense system based on Mobile agents by Eid et al. (2004)

Architecture

It comprises of the following components:

(i) Main Intrusion detection Processor
- Responsible for monitoring network segments (hosts) and acts as central intrusion detection and processing units
- Responsible for collection and correlation of IDS data from distributed IDS mobile agents.
- Acts as a secure, trusted repository for the mobile agents to obtain latest information about attacks that they should look forand to update the severity lists.

(ii) Mobile Agent Platform (MAP)

The MAP can create, interprete, execute, transfer and terminate/kill agents. The platform which is a small server program that resides on each host is responsible for accepting requests made by network users and generating IDS mobile agents plus dispatching them into the network to do intrusion detection functions.

(iii) Mobile IDS agent

Each host has a mobile IDs agent roaming all its hosts at all times. This agent is responsible for detecting intrusion based on data gathered by sniffing on the network traffic.

Data Collection

Data collection is from both the hosts and the main machine. It is done by the mobile agents that roam the network for IDS data.

Technique

The approach taken in this work can be categorized as misuse detection. Once logs are collected, the raw data is linked to structure for analysis by the detection engine. The detection engine processes the captured packets by checking them (the header and/or the content of the packet depending on the severity level) against a set of rules. If the rules match the data in the packets, then alerts are triggered and written into the output alert files and responses are sent to both the user interface and dispatched agents. The response to alert in this work is passive.

Strengths

The mobile agents in this work are fully managed and network resources utilization is saved when there is no attack.

Problems

High false positive rates, so many attacks could be missed when the severity level is between 3 and 5. Also, the security of the whole system is not discussed.

MAIDS - Architecture for distributed Intrusion detection using Mobile Agents by Li et al. (2004)

Architecture

Li et al. (2004) named their architecture MAIDS after the generic name for mobile agent-based IDSs. The architecture includes four components: Manager, Assistant Mobile agent, Response mobile agent and Host Monitor Agent. The host monitor agent which resides on every host cooperate three subagents namely network detection subagent (for network access), file detection subagent (for file operation) and user detection subagent for privilege operation. If the intrusion can be determined at certain monitored host, HMA reports the intrusion directly to the manager, otherwise it asks manager for aid and it only records the suspicious activity. The manager is the center for controlling and coordinating all other components. It maintains configuration information about all components including HMA, MA platform, Assistant MA, and Response MA. Manager is also responsible for creating, dispatching, accepting and removing MAs according to the host's request and environment.

Data Collection

The mode of data collection is not reported in this work but there are 3 categories of the types mentioned which are network access, file operation and privilege operation.

Technique

MA-IDS proposed a synthetic fuzzy analyzing method, where each activity is specified with a "suspicious level" and the suspicious level increases with the accuracy times of the activity. Each host that is ever connected to the network is assigned a suspicion level. These suspicion levels are stored into the interpretation base which can be changed with the analyzing results of the Intrusion Analyzer about intrusion increases (this process is called Learning). When an intrusion access is determined, the suspicion level of its source host and its user will be increased. According to Deeter et al. (2004), MAIDS explored the usage of dynamic agent composition technique to create an array of lightweight agents to perform a full range of IDS-related tasks.

Security of MA

An agent security module is designed based on the benefits of public-key cryptography, symmetric key cryptography and message authentication codes. Firstly, the agent is encrypted before it is transported between hosts using a symmetric key algorithm with a one time session key. This session key is then encrypted using a public key algorithm, implementing the authentication of the other side to the originator. The MAC is computed for receiver to verify the integrity of the agent upon arrival.

Strengths

The evaluation criterion is based on 3 categories: Intrusion detection ability evaluation which reported that 94.1% attacks can be detected. The system performance evaluation is also taken where the use time of CPU is less then 1% and approximately 5% memory is exhausted and lastly, the mobile agent performance is taken where the interval from the departure of Host Monitor agent or Manager to their return is taken. It was reported that it took a long time that agents migrated with authentication and encryption though the transportation of these agents was very fast.

Problems

The security of the location of the manager is not reported, hence if this is found by attackers, the IDS would be in a dangerous situation.

APHIDS - A Mobile Agent-based Programmable Hybrid Intrusion Detection System by Deeter et al. (2004)

Architecture

APHIDS employs a network-based architecture by placing an agent engine at every location. It is realized as a distributed layer which operates on top of a set of distributed agent engines. APHIDS architecture takes the advantage of the mobile agent paradigm to implement a system capable of efficient and flexible distribution of analysis and monitoring tasks, as well as integration of existing detection techniques.

Data Collection

The architecture delegates data capture and detection tasks to existing monitoring systems which are host and network.

Security

The security of the agents is not considered.

Technique

A trigger event is an abstract concept that simply refers to any suspicious event occurring on the network. A trigger agent is programmed to detect. A collection of Distributed Correlation Script which associates a trigger event with a series of analysis tasks to be performed when an event is detected, is provided as input to the system. Distributed search and analysis are implemented with mobile agents.

Strengths

APHIDS makes its Analysis Agent lightweight in order to save the bandwidth during the transfer of log data. The use of Distributed correlation scripts in capturing the expert knowledge of security administrator by automating the standard investigative procedures that are performed in response to an incident.

Problem

The security of the agents is not considered.

IMA-IDS- Intelligent and Mobile Agent for Intrusion Detection System by Barika & El - Kadhi (2003)

Architecture

The architecture involves four agents which are cloned namely: Collector agent, correlator agent, analyzer agent and the manager agent charged with the following duties:

The Collector agent patrols the network and collects all the events occurring in the host to which it is related, that is, there is a specialized collector agent for a category of event. The correlator agent gathers the critical information and sends it to the appropriate analyzer agent. The analyzer agent analyzes based on some methods, then reports the result to the manager and it now generates alarms if they detect any anomaly. The Manager agent gathers collected information and distributes to the analyzer agent. To be able this keeps track of all created and running agents.

Data Collection

Both network and host based.

Security

The security mechanism is based on Aglet Framework which uses an asymmetric cryptography system to exchange private keys between hosts. These keys ensure agent identities when transferred over the network.

Technique

As at the time of development of this work, the analysis techniques are under development. Though the model proposed is based on compartmental and statistical functions.

Strength

The agents are well distributed and the communication protocol is well defined.

Problem

There could be problem if an attacker has an indepth knowledge of the cryptography system by Aglet's framework.

Sparta - Applying Mobile Agent Technology to Intrusion Detection by Krugel and Toth (2000)

Krugel and Toth (2000) developed a system called Sparta (an acronym for Security Policy Adaptation Reinforced Through Agents) whose primary aim is to detect security violations in a heterogeneous, networked environment.

Architecture

Each host has at least a local event generator, a storage component, and the mobile agent platform. The local event generation is done by sensors which monitor interesting occurrence on the network or at host itself. Snort (an intrusion detection system) is used to extract interesting events from network traffic. The events are stored in a local database for later retrieval.

Data Collection

The source of data collection as reported by the authors is host-based.

Security

Sparta utilizes an asymmetric (public/private key pair) cryptosystem to exchange private keys which are needed to secure agents when they are transferred over the network. The agent code is signed and can be authenticated before it is executed (to protect the platform). The signature is also used to determine the set of permissions an agent is granted when executing on a platform

Technique

The method used in this work is correlation mechanism which follows a distributed approach. When detecting patterns, agents first try to find actual events which are specified by the root node of a given tree pattern. When the root node is located, the agents follow the branches of the tree to detect events that match the root's predecessors. This process is recursively applied until the whole tree has been matched. Sparta uses mobile agents to provide a query like functionality to reconstruct patterns of related events distributed across multiple hosts.

Strengths

The algorithm allows very few data to be carried by agents during hop, this could improve the performance of the mobile agents being lightweight.

Problems

Bandwidth Scalability: The bandwidth required to collect large, distributed data sets from distributed sensors can pose a significant overhead cost, affecting network performance.

Based on the feature in the classification of IDS, Table 1 summarizes the review of MA-IDSs

Table 1: Summaries of reviewed MA-IDSs

S/N	Authors	Approach	Source of data	Security of Mobile Agent	Technique
1.	**Abraham et al. (2007)**	Hybrid	Network based	Not considered	Soft computing paradigm
2.	**Sodiya (2006)**	Misuse detection	Network based	Based on Aglet framework in addition to Recorded state mechanism	Modified Apriori Algorithm
3.	**H. Q. Wang et al. (2006)**	Hybrid	Hybrid	Based on Aglet framework	Rule based method
4.	**Eid et al. (2004)**	Misuse detection	Both host and main machine	Not discussed	Correlation analysis
5.	**Li et al. (2004)**	Hybrid	Hybrid	Public key cryptography	Fuzzy analyzing method
6.	**Deeter et al. (2004)**	Hybrid	Hybrid	Not considered	Distributed Correlation Scripts
7.	**Barika & El - Kadhi (2003)**	Anomaly	Hybrid	Based on Aglet framework	Compartmental and statistical functions
8.	**Krugel and Toth (2000)**	Hybrid	Host based	Asymmetric cryptosystem	Correlation mechanism

Suggested Considerations for Improved MA-IDS

Eid (2005) suggested that the following three categories of research on using mobile agents with IDS should be considered

- New detection paradigm: The techniques used for detecting intrusion should be improved.
- New architecture paradigm: Is it hierarchical IDS architecture, network IDS architecture or Hybrid IDS architecture?
- Improvements to existing design: How is the system reducing false alarm rates?In order to overcome the shortcomings of the existing MA-IDSs, this paper proposes some suggestions for an enhanced MA-IDS based on the following features:

1. **Architecture**: With reference to the section that discusses classification of IDS, hierarchical architecture is rigid in nature because of the precise functioning and lines of communication that tend to become associated with their components. According to Jansen et al. (1999), network architecture tends to suffer from inefficiency in communications because of the unconstrained communication flow. As a way of incorporating the best characteristics of hierarchical and network architectures, **a hybrid model** which allows free communication as discussed in Abraham et al. (2007) is hereby proposed.
2. **Approach** : An anomaly-based IDS will lead to high false positives, in order to solve this problem a hybrid approach (combining both misuse and anomaly) is proposed.
3. **Source**: Network and Host based
4. **Security** of Mobile Agent ; According to Jansen et al. (1999) "If a MA-IDS system can restrict processing to only those agents digitally signed by a security administrator, it greatly reduces the security vulnerabilities, since an attacker can not change the code of an agent to cause it to be malicious". A fundamental technique for protecting an agent system is signing code or other objects with a digital signature. A digital signature is an electronic analogue of a written signature; it serves as a means of confirming the authenticity of an object, its origin and its integrity. Digital signature techniques compared to other techniques for securing mobile agents can be used to provide assurance that the claimed signatory signed the agent i.e. for the authentication of the mobile agent and it can be used to detect whether or not the agent was modified after it was signed i.e. to check the integrity of the mobile agent. In light of this, **Digital Signature Algorithm** is hereby suggested for securing mobile agents.
5. **Technique**: Data mining for intrusion detection with focus on **extracting closed frequent patterns**.

Hui et al. (2004) designed an algorithm for mining maximal frequent itemset (M) in intrusion detection system in order to significantly improve the performance of an IDS. According to Zaki (2006) "… $M \subseteq C \subseteq F$ where closed itemset is being denoted as C and frequent itemsets as F". This implies that closed frequent itemset is larger than the set of maximal frequent itemsets. In this case, extracting the closed frequent patterns will reduce the false alarm rates which might have been missed by maximal itemsets and could have been more from frequent itemsets. (See Ibrahim et al., 2005 for more illustrations on closed frequent itemsets.)

Conclusion and Future Works

In this paper, we proposed a novel classification of a typical intrusion detection system. Based on the features proposed which are architecture, mode of data collection, the approach to detection, the security and the techniques, we have critically reviewed some existing MA-IDSs. It is noted

that some of these existing systems are still faced with drawbacks and some with strengths. Based on the strengths and weaknesses, we outlined some suggestions for enhanced MA-IDSs. The implementation is on, using the IBM Aglet platform and Sun's Java development kit 1.1.8. Being java based, it will run on any java enabled device. At present, we have integrated all the suggestions made in the section above into our model. We plan to publish the result on testing with the KDD cup 1999 dataset in our next paper.

References

Abraham, A., Jain, R., Thomas, J., & Han, S. Y. (2007). D-SCIDS: Distributed soft computing intrusion detection system. *Journal of Network and Computer Application*, *30*, 81-98.

Almgren, M., Barse, E. L. & Jonsson, E. (2003). Consolidation and evaluation of IDS taxonomies. *Nordic Workshop on Secure IT Systems (NordSec 2003)*, pgs 57 -70, Norway, Oct. 2003.

Anderson, J. P. (1980). *Computer security threat monitoring and surveillance*. Technical report, James P. Anderson Co., Box 42, Fort Washington, February 1980.

Bace, R., & Mell, P. (2002). *Intrusion detection system*. Technical report, NIST Special Publication on Intrusion Detection, 2002.

Balasubramaniya, J., Garcia-Fernandez, J. O., Isacoff, D., Spafford, E. H., & Zamboni, D. (1998). An architecture for intrusion detection using autonomous agents. *Proceedings of 14th Annual Magnetism Computer Security Application Conference*, Phoenix, USA, Dec. 1998.

Barika, F. A., & El - Kadhi, N. (2003). Intelligent and mobile agent for intrusion detection system. *Proceedings of International Conference of Information and Communication Technology*, Egypt, Nov. 2003.

Chan, P. C., & Wei, V. K. (2002). Preemptive distributed intrusion detection using mobile agents. *Proceedings of 11th IEEE International Workshops on Enabling Technologies*. June, 2002, pp. 103 – 108.

Deeter, K., Singh, K., Willson, S., Filipozzi, L., & Vuong, S. (2004). *APHIDS: A mobile agent- based programmable hybrid intrusion detection*. Retrieved from http://www.cc.gatech.edu/grads/k/ksingh/publication/aphids_cameraready.pdf

Eid, M., Artail, H., Kayssi, A., & Chehab, A. (2004). An adaptive intrusion detection and defense system based on mobile agents. *Proceedings of the Innovations in Information Technologies (IIT'2004)*, Oct, 2004, Dubai, UAE.

Eid, M., Artail, H., Kayssi, A., & Chehab, A. (2005). Trends in mobile agent application. *Journal of Research and Practice in Information Technology*,*37*(4).

Hui, W., Qing-Hua, L., Huanyu, X., & Sheng-Yi., J. (2004). Mining maximal frequent itemsets for intrusion detection. *International Workshop on Information Security and Survivability for Grid (GISS'2004)*, Vol. 3252, 2004.

Ibrahim, S. A., Folorunso, O., & Ajayi, O. B. (2005). Knowledge discovery of closed frequent calling Patterns in a telecommunication database. *Proceedings of the 2005 Informing Science and IT Education Joint Conference, Flagstaff, Arizona, USA. pp 137 – 148*. Retrieved from http://proceedings.informingscience.org/InSITE2005/P13f80Ibra.pdf

Jansen W., Mell, P., Karygiannis, T., Marks, D. (1999). *Applying mobile agents to intrusion detection and response*. An NIST interim report article, October 1999.

Kruegel, C., & Toth, T. (2002). *Applying mobile agent technology to intrusion detection*. Technical Report Number TUV-1841-2002-31, Technical University of Vienna.

Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A data mining framework for building intrusion detection models. *Proceedings of the 1999 IEEE Symposium on Security and Privacy Oakland, California*, pp 120 - 132.

Li, C., Song, Q., & Zhang, C. (2004). MA-IDS: Architecture for distributed intrusion detection using mobile agents. *Proceedings of the 2nd International Conference on Information Technology for Application (ICITA, 2004)*.

Sodiya, A. S. (2004). *A new combined strategy for intrusion detection*. Ph.D. Thesis, Department of Mathematical Sciences, University of Agriculture, Abeokuta, Nigeria.

Sodiya, A. S. (2006). Multi-level and secured agent-based intrusion detection system. *Journal of Computing and Information Technology, 14*(3), 217-223.

Wang, H. Q., Wang, Z. Q., Zhao Q., Wang G. F., Zheng R. J., & Liu, D. X. (2006). Mobile agents for network intrusion resistance. *APWeb Workshops 2006*, LNCS 3842, pp 967-970.

Wang, W., Behera, S. R., Wong, J., Helmer, G., Honavar, V., Miller, L., Lutz, R., & Slagel, M. (2006). Towards the automatic generation of mobile agents for distributed intrusion detection system. *Journal of Systems and Software, 79*, 1-14. Retrieved from www.elsevier.com/locate/jss

Zaki, M. J. (2006). 6.1 frequent pattern mining. *A lecture note on Data Mining*, Edited by M. Li, J. Ouyang, and Z. Xie.

Biographies

Onashoga, Saidat Adebukola (nee OKUNLAYA, formerly IBRAHIM, S. A.) is a lecturer in the Department of Computer Science, University of Agriculture, Abeokuta, Nigeria. She is currently on her Ph.D. programme in Computer Science in the same University. She has published in both International and local journals. Her current research interests include Intrusion Detection, Data Mining and Computer Security.

Adebayo D. Akinde is an associate professor in the department of computer science, University of Agriculture, Abeokuta Ogun State. He had supervised several M.Sc. and Ph.D students in computer science. His areas of research interests include modelling and simulation, mobile agents technology and e-commerce.

Sodiya, Adesina Simon is presently a senior lecturer in the department of Computer Science, University of Agriculture, Abeokuta. He has a Ph.D. in computer science. He has published in both local and international journals. His research areas are Computer Security, Artificial Intelligence, Software Engineering, and Data mining.