International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:9, 2008

A Novel Hybrid Mobile Agent Based Distributed Intrusion Detection System

Amir Vahid Dastjerdi, and Kamalrulnizam Abu Bakar

***Abstract*—**The first generation of Mobile Agents based Intrusion Detection System just had two components namely data collection and single centralized analyzer. The disadvantage of this type of intrusion detection is if connection to the analyzer fails, the entire system will become useless. In this work, we propose novel hybrid model for Mobile Agent based Distributed Intrusion Detection System to overcome the current problem. The proposed model has new features such as robustness, capability of detecting intrusion against the IDS itself and capability of updating itself to detect new pattern of intrusions. In addition, our proposed model is also capable of tackling some of the weaknesses of centralized Intrusion Detection System models.

***Keywords*—**Distributed Intrusion Detection System, Mobile Agents, Network Security.

I. Introduction

THERE document There are two ways to protect our network against malicious attempts. First is to build complete secure network system by applying all complicated cryptographic, authentication and authorization methods. However, this solution is not realistic. In practice, it is impossible to have completely secure system, because inside the system the user usually used operation system and other applications which have vulnerabilities. Second is to detect an attack as soon as possible preferably in real-time and take appropriate action. This is essentially what an Intrusion Detection System (IDS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active. However, IDS which uses mobile agents are new class for intrusion detection system.

Mobile agents can be defined as "self-contained and identifiable computer autonomous programs, bundled with their code, data, and execution state that can move within a heterogeneous network of computer systems. They can suspend their execution on an arbitrary point and transport themselves into another computer system." [1]. Mobile agents have special characteristics which can help intrusion detection in several ways. The used of mobile code and mobile agents computing paradigms have been proposed in several researches [2, 3, 4]. The advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adopting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior.

Amir Vahid Dastjerdi is a student of Centre for Advanced Software Engineering, Universiti Teknologi Malaysia, City Campus, Jalan Semarak, 54100 Kuala Lumpur, Malaysia (e-mail: Vahid.av@gmail.com).

Kamalrulnizam Abu Bakar is with Faculty of Computer Science & Information System, Universiti Teknologi Malaysia, 81310 UTM Skudai, Johor D. T, Malaysia (e-mail: knizam@utm.my)

II. Related Works

Most of mobile agent based intrusion detection systems, such as Autonomous Agents for Intrusion Detection (AAFID) [9], follow a hierarchical structure.

In this type of IDS, data is collected both at the host and network levels by reviewing audit trails and/or monitoring packets in a network. All collected data are sent to the central data coordinator. The coordinator then analyzes all the information received to decide the status of the system, and actions that need to be taken. The mentioned system can perform intrusion detection task, however it is vulnerable. If any part of the internal nodes (or even the root node) is disabled, the functioning of that of branch of IDS will be disqualified. In addition they are not flexible, and not completely distributed. Furthermore, in those hierarchical models no approach has been taken to respond to attack against intrusion detection system itself. As a result, if intruder can gain access to IDS coordinator (IDS control center), the whole system will be affected. The performance of IDS with mobile agents is considerably relying on the produced network load by the agents.

III. Our Proposed Hybrid Model Design

The proposed hybrid model design is inspired by two models namely peer to peer IDS based on mobile agents [5] and distributed intrusion detection using mobile agents (DIDMA) [8]. Mobile agents are by nature autonomous, collaborative, self-organizing, and mobile. These attributes enable IDSs to implement completely new approaches for doing intrusion detection, some of which are based on analogies found in society and in nature.

A Society based analogy has been used in our proposed model. Societies encompass neighborhoods, and neighborhoods are composed of families. Likewise, networks include subnets and each subnet of network consists of computers. In our hybrid model design, there is an IDS control center in each subnet, which plays role comparable to parents in family. In a family, parents are responsible to watch after children, and similarly IDS control centers are responsible to

look after hosts in subnet. In addition, families in the same neighborhood usually take care of each others properties to make the neighborhood safer. Likewise, in our proposed hybrid model design the IDS Control Centers in each virtual neighborhood are assigned a task to keep an eye on each others.

A. Components of the IDS in a Subnet

The fundamental design of our proposed hybrid model in each subnet consists of four main components namely IDS Control Center, Agency, Static Agent Detectors, and Specialized Investigative Mobile Agent Detectors.

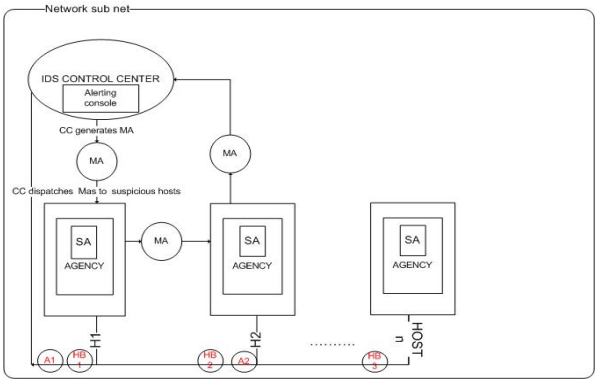

Fig. 1 IDS Architecture in a Subnet

As can be seen from the Fig. 1, Static Agents(SA) should generate alert whenever they detect suspicious activities, then save those activities information in log file and send alert's ID (like A1 in the Fig. 1) to IDS control center. Then, IDS Control Center will send investigative task-specific mobile agent to every agency that sent similar alerts (which are Host 1 and Host 2 in our example). As shown in the Fig. 1, MA will visit and investigate all those hosts, collect information from them, correlate the information and finally send or carry back the result to IDS control center. Consequently, Alerting Console in IDS Control Center will analyze the coming information and compare and match with intrusion patterns in IDS CC database then it will raise the alarm if it detects an intrusion. IDS Control Center then saves the information received from investigative MA into its database for later usage and investigation. Names and identifications of possibly discovered compromised hosts will be black listed and sent to all hosts except the black listed hosts. As a result, other hosts will stop communicating with the hosts in the black list. As depicted in Fig. 1, in this application every Host should transmit an "I'm alive" heart beat (shown as HB in Fig. 1) message to the IDSCC at regular intervals to indicate their status. In cases when these messages are not received, the IDSCC assumes that the Host is attacked.

1) Agency

Mobile Agents need an environment to become alive. That environment is called Agency. An agency is responsible for hosting and executing agents in parallel and provides them with environment so that they can access services, communicate with each other, and migrate to other agencies. An agency also controls the execution of agents and protects the underlying hardware from unauthorized access by malicious agents.

2) Static Agent Detectors

Static Agent Detectors (SAD) act like host monitors, generating ID events whenever traces of an attack is detected, and these events are sent in the form of structured messages to IDS Control Center [8]. For example, when SAD identifies failed password guessing attempts as a suspicious activity, an ID event is generated to check for corresponding attack. SAD is capable of monitoring the host for different classes of attacks. The SAD is responsible for parsing the log files, checking for intrusion related data pattern in log files, separating data related to the attack from the rest of the data, and formatting the data as required by the investigative MA. The architecture of our IDS allows applying components of other project as an intrusion detection sensor. In that case static agent detectors will work on top of those sensors. For instance the SNORT [6] network intrusion detection system and its sensors can be used to do packet filtering and looking for intrusion signatures in the packets.

3) Investigative Mobile Agents

Investigative Mobile agents (IMA) are responsible for collecting evidences of an attack from all the attacked hosts for further analysis. Then, they have to correlate and aggregate that data to detect distributed attacks. Each IMA is only responsible for detecting certain types of intrusions. This makes it easier for updating when new types of intrusion is found or new types of detection method is invented. In addition, it lets Mobile agents carry less data and code. In addition, the IDS can also be updated and extended by adding new MAs. The investigative MA uses List of Compromised Agency (LCA) to identify its itinerary for visiting Hosts.

4) IDS Control Center

An Intrusion Detection System Control Center is a central point of IDS components administration in each subnet. It includes following components:

- Databases: there should be a database of all intrusion patterns which can be used by Alerting Console to raise the alarm if patterns matched with the detected suspicious activities. All events IDs which reported by SA are stored in another database. In addition all related system logs should be stored in a database as well.
- Alerting Console: this component compare the spotted suspicious activity with intrusions' database and raise the alarm if they are matched.
- Agent generator: functions to generate task specific agent for detecting intrusions even new ones by using knowledge that is generated by data mining inference engine or obtained from previous experience.
- Mobile agent dispatcher: dispatched investigative mobile agents to the host based on the ID of event or suspicious

activity received from their static agents. In addition it determines list of compromised Agencies (LCA) for investigative MAs.

- Data mining inference engine: uses machine learning to deduce knowledge to detect new intrusions from System databases which contains detected intrusion and system logs and coming information from SAs.
- Trust level manager: defines trust level for all agencies in the subnet, furthermore it keep the trust level of the other IDS Control Centers in the same neighborhood of network.

The overall structure of IDS Control Center is illustrated in Fig. 2:

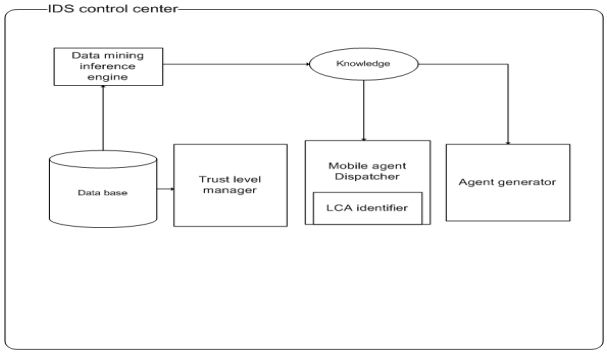

Fig. 2 IDS Control Center Architecture

As can be seen from the Fig. 2, data mining technique is included in the design. The main reason of applying data mining in our design is to acquire knowledge to discover new intrusion patterns and also to decrease false alarms. Applying data mining, information can be converted into knowledge on historical patterns and future trends. For example, summary information on histories of intrusion and system calls and logs can be analyzed in light of promotional efforts to provide knowledge of distributed cooperative intrusive behavior. As can be figured out from Fig. 2, the achieved knowledge can help agent generator to generate new type of investigative Mobile agents, which are capable of detecting new types of intrusion. On the other hand, Data mining inference engine uses machine learning to acquire new predictive rules for detecting new intrusion patterns as well.

Trust level of all agencies in the subnet can be modified by the Trust level manager. For example, as mentioned earlier in this paper in the case of the heart beat messages are not received by IDSCC from an Agency, trust manager will decrease the trust level of the Agency. However, when trust level of the Agency reached specific threshold, it will be identified as a compromised Agency.

The other important issue is in defining List of Compromised Agencies (LCA). As pointed out, all hosts which produced same suspicious activity ID will be included in the same LCA. However, when a host gets breached there is high probability that its neighbors are in risk too and consequently, they have to be investigated as well. Our approach for defining the LCA is by using a simple version of the Graph based Intrusion Detection system (GrIDS) [7]. The GrIDS generates different shapes of graphs for a period of time that is an indication of large scale distributed attack. The nodes and the links of the graph represent the suspicious machines and the connection between the machines respectively. The further propagation of the attack to other machines leads the way to the growth of the graph. This graph representation is then summarized to produce results that are compared with threshold values for an indication of an attack. Meanwhile, acquired knowledge may lead to fined new pattern of attack propagation as illustrated in Fig. 2.

The current IDS is efficient in detecting intrusions in hosts within the sub-network by IDS CC. In order to deal with this problem we are going to apply neighborhood watching solution in the IDS application.

B. Neighborhood Watching Scenario for Detecting Intrusion on IDS CC

Neighborhood watching [5] approach is inspired by the real world where neighbors cooperate with each others to achieve more secure neighborhood. In this approach, all neighbors have the task to watch out for each other belongings. Everyone knows his neighbors usual behaviors. Whenever suspicious behaviors of neighbors are spotted, the neighbor where the incident occurred and other interested parties such as police will be informed. As a matter of fact, living in such community is safer.

In order to apply that system to our IDS application, the first step is building a virtual neighborhood where all IDS Control Centers are peers in the same neighborhood. When any new IDS Control Center enters into the system, it has to be assigned a neighborhood. The configuration of this neighborhood system is not fixed and can be dynamic. The initial configuration encompasses a graph of nodes and their location in the network defines the neighborhood. In order to get the efficient performance the number of neighbors in each neighborhood should not exceed a predefined upper bound.

In this neighborhood watch approach all IDS CC are considered to be equal. Every IDS CC will perform intrusion detection for other IDS CC in its neighborhood. In a neighborhood, each Control Center stores data about its neighbors mainly the description of normal behavior of the neighbors and information such as checksums of critical operating system files. As an example, if Host A detects intrusion in neighbor B then it will negotiate with B's neighbors. Consequently, if consensus is obtained then Host B will be identified as a Compromised neighbor.

In order to show how the system works, a threat scenario will be proposed and then system reaction to that threat will be explained. Firstly, it should be explained that for all IDS CC a trust level was defined for all of its neighbors. Whenever trust level falls below critical level it shows that the IDS CC is compromised. Let assume the following scenario: Host A as illustrated in Fig. 3 has Hosts B, C, and D as its neighbors. Therefore it should keep some information about its neighbors. Host A dispatcher sends out investigative Mobile

Agent which is specialized in detecting specific kind of intrusion to Host B. After those checks MA returns to Host A and report its finding. The IDS CC in Host A compares this report with what it has in its database, if Host B behavior does not match with the information in its database, there might be an intrusion. Therefore, Host B trust level falls below the critical level. Then, IDS CC in Host A sets off a voting ballot and sends it to Host B neighbors that are Host C and D.

The IDS CC in Host C receives the ballot, and check its trust level on Host B, and based on that information votes and passes the ballot on to Host D. IDS CC in Host D in the same way votes and passes it back to Host A. IDS CC in Host A receives the ballot and if it recognizes that majority votes against Host B, Host A will put Host B in its Black List and send the Voting result to all Host B's neighbors and obviously the neighbors will take appropriate action to protect themselves against Host B.

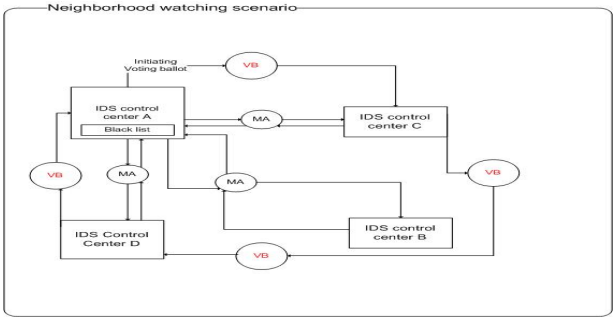

Fig. 2 Neighborhood watching scenario

As shown, attacks on IDS CC are detectable using the peer to peer model. Consequently we successfully accomplished the ring of protection in our network. Our proposed hybrid model for intrusion detection system seems to be more robust than each of the applied model individually. Furthermore, it tackles the single point of failure problem in the AAFID model because there are more than one IDS CC in a network. In addition, network latency issue is solved and network load is also distributed more symmetrical among the network. Moreover, using data mining and knowledge acquiring techniques our model is even capable of achieving new knowledge to detect new kind of intrusion.

IV. Discussion

As mentioned in the section III.A.3, mobile agents are used in our model for investigation of Hosts in a subnet. In order to give them ability of investigation in remote hosts, they should be granted a permission of accessing the Hosts resources like file system, network interfaces, and so on. There are two options, first is to give them every right to access all resources (which is the easiest way, but totally against computer security principals). Second approach is to restrict their access to the resources which they need for investigation. The second approach is also used in real life. Whenever police is intended to investigate a place, first they should ask a judge to issue a certificate of an investigation for them. And they can only investigate the places that mentioned in a certificate. This approach is also applicable in our model. Therefore, IDS Control Center instead of a judge should issue a certificate which will authorize a mobile agent to access to certain resources on remote Hosts.

However, it should be mentioned that Intrusion detection systems which use mobile agents take over the immaturity of mobile agents toolkits such as security architecture flaws. Consequently, further development of mobile agent's toolkits will make it easier to apply them into IDS systems.

V. Conclusion and Further Works

The paper aim is in building up robust distributed IDS which covers the flaws of the other models while uses their useful features. In conclusion, The Hybrid design could even detect attack against IDS control centers while agents roam through the network to spot intrusions. Nonetheless, weaknesses are unavoidable in a new design, and many areas discussed in this paper would benefit from further efforts to clarify the design fine points and implementation details. Further work should also look into mobile agent's intercommunication and negotiation which can help investigative mobile agents to share their knowledge. In addition intrusion pattern's knowledge sharing between IDS control centers can be considered for further studies.

Acknowledgment

This research is supported by the Universiti Teknologi Malaysia (UTM).

References

[1] Peter Braun, Wilhelm R. Rossak, Mobile Agents: Basic Concepts, Mobility Models, and the Tracy Toolkit, published by Morgan Kaufmann (December 22, 2004), ISBN-10: 1558608176.
[2] Andreas Fuchsberger, "Intrusion Detection Systems and Intrusion Prevention Systems"; Information Security Group, Royal Holloway, University of London, Egham, Surrey TW20 0EX, United Kingdom 2005.
[3] J. P. Anderson. Computer Security Threat Monitoring and Surveillance. Technical Report, James P. Anderson Co., April 1980.
[4] Richard A. Kemmerer and Giovanni Vigna, Intrusion detection: a brief history and overview Reliable Software Group, Computer Science Department, University of California Santa Barbara 2003.
[5] Geetha Ramachandran and Delbert Hart, A P2P Intrusion Detection System based on Mobile Agents, 2004 ACM 1-58113-870-9/04/04.
[6] Snort, (Oct 2005). Online. http://www.snort.org/,(March 2007).
[7] S.Stainford-Chen, Steven Cheung, et.al. GrIDS-Graph Based Intrusion Detection System for Large Networks. In the Proceedings of the 19th National Information Systems Security Conference, Baltimore, MD, October 1996.
[8] Pradeep Kannadiga and Mohammad Zulkernine School of Computing Queen's University, Kingston Ontario, Canada K7L 3N, DIDMA: A Distributed Intrusion Detection System Using Mobile Agents, 2005 IEEE.
[9] J.Balasubramainyan, J.O. Garcia-Fernandez, D.Isacoff, E.H. Spafford, D.Zamboni, An architecture of intrusion detection using autonomous agents, Department of Computer Science, Purdue University coast TR 98-05, 1998.