3

A Sustainable Component of Intrusion Detection System using Survival Architecture on Mobile Agent

Sartid Vongpradhip, Ph.D., and Wichet Plaimart
Chulalongkorn University, Rajamangala Thanyaburi University of Technology
Thailand

1. Introduction

The rapid growth of the Internet uses all over the world, estimation from the statistics up to December, 2010 [1], found that there are 6,845 Million Internet users worldwide. However, it comes with problems about threats; especially the Distributed denial-of-service attack (DDoS) that make the victim cannot services as usual. This threat is one of the computer network security problems that attack the confidentiality, authentication, integrity, non-repudiation, access control, and availability [2]. The major objective of these types of attack is to make the victim cannot access the resource or service the user as usual [3]. Those problem not only important for the security of the organizations network, but also can cause those organizations cannot connect to the Internet connection, especially if that organization having the transactions via the Internet, this will cause the huge effect that is hard to forecast. Moreover, nowadays there is still no method that can completely prevent or avoid those attacks [4]. IDS is defined as [5] the problem of identifying individuals who are using a computer system without authorization (i.e., 'cracker') and those who have legitimate access to the system but are abusing their privileges (i.e., the 'insider threat'). For our work, we add to this definition the identification of attempts to use a computer system without authorization or to abuse existing privileges. Thus, intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource".

IDS acts like the gate-keeper that has a duty to screen the people who come in and out the network. It will detect and block the intruder to access the network, therefore one of the objectives of IDS is to classify correctly between the real intrusion activity and the activity that similar to the intrusion but not the intrusion. Now, IDS is the software that detects, specifies, and reacts on the activities without the permission or the activities that are unusual on the target system. Various form of IDS are use as the main tool to detect and protect all of the computer system resources in the organization, may be the specific tool or the software that can install on the system that need to be protected.

Furthermore, IDS is used as the major tool in the detecting and preventing the computer network resources in the organizations. So, IDS is the first target that the intruder will be attacked. I they can make IDS not convenient; all of the computer network resources have no prevention. However, as we cannot avoid the attack, the problem is how we can survive from the attack. For that, we must design the intrusion detection system that is based on the

basic of the architecture that is durable and can survive when there is an attack. So, the research about the intrusion detection system architecture design which is durable is the challenge.
The content in this paper divided into 7 sections. Firstly, the section is introduction. Secondly, the section is the related work. Thirdly, this section will explain about our architecture and model description. Fourthly, the section is architecture analysis. Fifthly, the section is analytical result. Sixthly, the section is our architecture proofing. And the last section is conclusion, recommendation and future work.

2. Related work.

The research in the field of the intrusion detection system that use the agent-based detection representative program technology can be separated to 3 levels, approach level [6], [7], [8], [9], [10], [11] implementation level [12], [13], and evaluation level [14], [15]. At present, the research about the technology of the Mobile Agent that uses the intrusion detection system is rapid growth. From our study the present IDS in the both of commercial and research, we found that most IDS use the architecture that has hierarchical structure that has both host-based and network-based sensor, which collect the data, fundamental compile and pass on the result from the server that is the central analyzer. Here is the conclusion of the intrusion detection system main problem.
Firstly, the single point of failure, the server that use for system analysis can found the single point of failure, if the intruder can make the server cause problem, slower or fail, for example, attack with DDoS. The system will have no protection.
Secondly, the scalability problem, the architecture that compile with one computer make the system cannot be larger, because the analyzer unit that use to analyze the system will be limited with the size of the network that is detected. Moreover, the process that the server must handle the communication from many other hosts, this not only causes the heavy traffic on the network, but also leads to the bottleneck too.
Thirdly, the difficulties of the adjusting of the configuration or ad the new abilities onto the components of the network, because mostly to the adjusting, correcting, and increasing the configuration, we must modify the configuration file, add or delete configuration file, or add new modules. These kinds of actions must restart the system, so the IDS can be used. Even if the third problem had been solved by implementing the mobile agent technology in the IDS architecture, however, the first two problems still not solved indeed.
In summary, the major problem of current IDS is not resistant to the attack of the IDS. This consequence from structural weaknesses of the lack of robust IDS that, lack of dynamic elements that can not escape the attack and lack of rapid backup and recovery mechanism.

3. Overview of our proposed architecture

This research goes to the effort to design the IDS architecture that is durable and survived after the attack. It is mainly use mobile agent technology to design and let IDS has more ability to the Distributed IDS.
In this research, we interest in the architecture design that still has the detecting function and response to prevent the computer system resource, but durable from the attack and survived by using mobile agent technology with the network topology design. To deals with the ability to be the Survival architecture for IDS, the design will be based on the topics as bellow.

3.1 Survival architecture.

Our conceptual framework to design for survival architecture based on highly available service of fault tolerant model which the model and description as the bellow.

A. Highly available service of fault tolerant model.

Our design concept based on highly available service of fault tolerant model. The framework for implementing highly available service by replicating data close to the points where group of clients need it. The replica manager exchange messages periodically in order to convey the update they have each received from clients. The service model provides two basic of operations: queries are read only operations and update modify but do not read the state. A key feature is that front ends send queries and updates to any replica manager they choose any that is available and can provide reasonable response time [18]. The system as shown in Fig. 1 make two guarantees, even though replica manager may be temporarily unable to communicate with one another, each client obtains a consistent service over time - or- relaxed consistency between replicas.

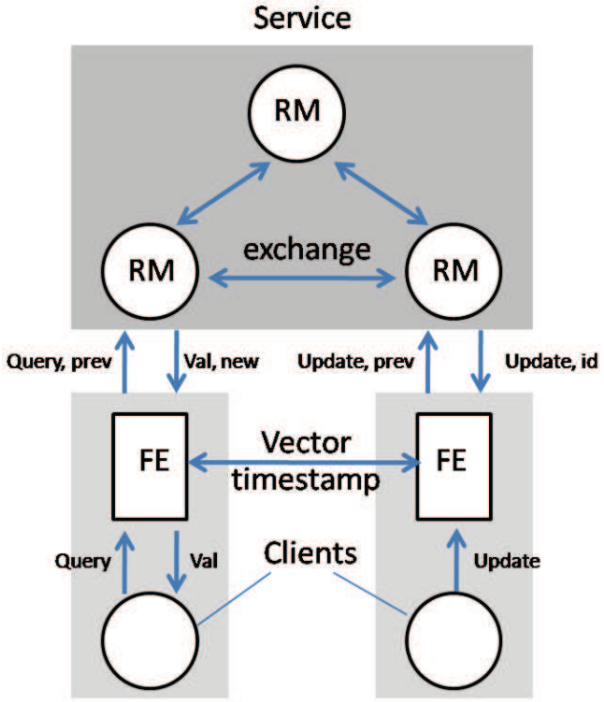


Fig. 1. Highly available service of fault tolerant model

The highly available service is a fault tolerant model that ability of the system will continue to work in conditions that damage occurred. The goal of a durable system of corruption is preventing failure of the system as possible. There have key three properties [18]; fault avoidance, fault masking and fault tolerance. Fault Avoidance is a technique to avoid damage that may occur. Avoiding damage is in the form of IDS architectural design. We use this property as a separate architectural design system divided by the critical resources of

the network into three sections includes Critical asset, Proxy partition and region. The enterprise network perimeter by zoning to break the trust-host and untrust host separated to the mechanism used to secure appropriate.
Fault Masking is the process to prevent fault that occur not to affect overall system performance. Our design of system architecture and network zoning this property to hide the fault of some of the elements and use the rapid backup and recovery mechanism to work instead.
Fault Tolerance is the ability of the system will continue to work in conditions that damage occurred. The goal of a durable system of corruption is preventing failure of the system as possible. The architecture, we use several techniques designed to sustain damage, including fault detection, fault location, fault containment and fault recovery. These techniques can all work under the Mobile Agent technology.

B. The Model Description

To explain our basic replication model, how a model processes queries and update operations is as follows.
Request: The front end (FE) normally sends request to only a single replica manager (RM) at a time. A front end will communicate with a different replica manager when the one it normally uses fails or becomes unreachable. It may try one or more others if the normal manager is heavily loaded.
Update Response: If the request is an update then the replica manager replies as soon as it has received the update.
Coordination: The replica manager that receives a request does not process it until it can apply the request according to the required ordering constraints. No other coordination between replica managers is involved.
Execution: The replica manager executes the request.
Query Response: If the request is a query then the replica manager replies at this point.
Agreement: The replica managers update one another by exchanging the messages, which contain the most recent updates they have received.
In order to control the ordering of operation processing, each front end keeps a vector timestamp that reflects the version of the latest data values accessed by the front end or the client. This timestamp (prev in Fig. 1) contains an entry for every replica manager. The front end sends it in every request message to a replica manager, together with a description of the query or update operation itself. When replica manager returns a value as a result of a query operation, it applies a new vector timestamp (new in Fig. 1). Since the replicas may have been updated since the last operation. Similarly, an update operation returns a vector timestamp (update id in Fig. 1) that is unique to the update. Each return timestamp is merged with the front end's previous timestamp to record the version of the replicated data that has been observed by the client.

3.2 System architecture

Allocate all the network resources into parts as shown in Fig. 2. Each part will be composed of Critical asset, Proxy partition and region. In the Critical asset there is Critical host which include the important Application server and Critical IDS hosts. In Proxy partition, there are the proxy agents' multicast groups and the intermediate layer hosts or network elements. The communication between this internal component and the communication with the

Critical asset has to use the high-speed transmission line or the network backbone that is hard to be attacked and region means the leaf LAN in the network.

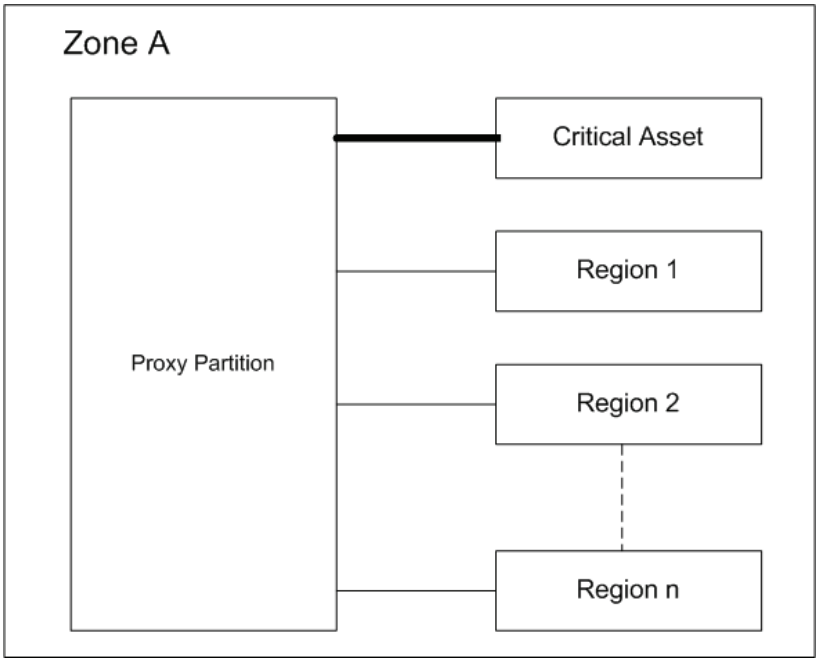


Fig. 2. System architecture

Using Proxy partition concept that has the proxy agent as the medium for the communication between the components for hiding the major resources from the approach an attack directly, having shadow agent as the redundancy mechanism and the backup and recovery mechanism design, makes the system durable for the attack and can be survived. Proxy agent in the proxy partition is the multicast group that composed of the group members; each group will have the shadow agent as the mirror group communicates with other groups. The objective of this structure is to make the shadow agent, uses for preventing the proxy agent as shown in Fig. 3.
Design the main components of the detection and response system is divided into groups, each group communicate by using the multicast group and asynchronous information transferring to reduce the amount of the information that are transferred in the network.

3.3 Enterprise network perimeter by zoning

The designs that will be divide all of organization's network resources into separate parts, according to the separate design concept as shown in Fig.4. Define the region of the network to support both trusted-hosts and untrusted-hosts. The network will be dividing to 4 zones, external network zone, internal network zone, wireless zone and DMZ (Demilitarized zone), as shown in Fig. 4 and has monitoring zone with the use of the network topology that has NAT (Network Address Translation) technique to hide the network resources from the outsider.

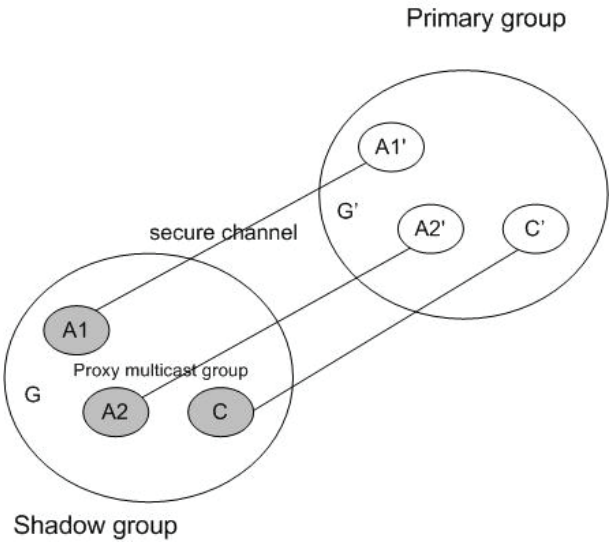


Fig. 3. Proxy agent and shadow agent

Although designed for corporate network security, this is actually not new. But today, most organization's network still does not focus much. They remain vulnerable to intruders use to attack at any time.

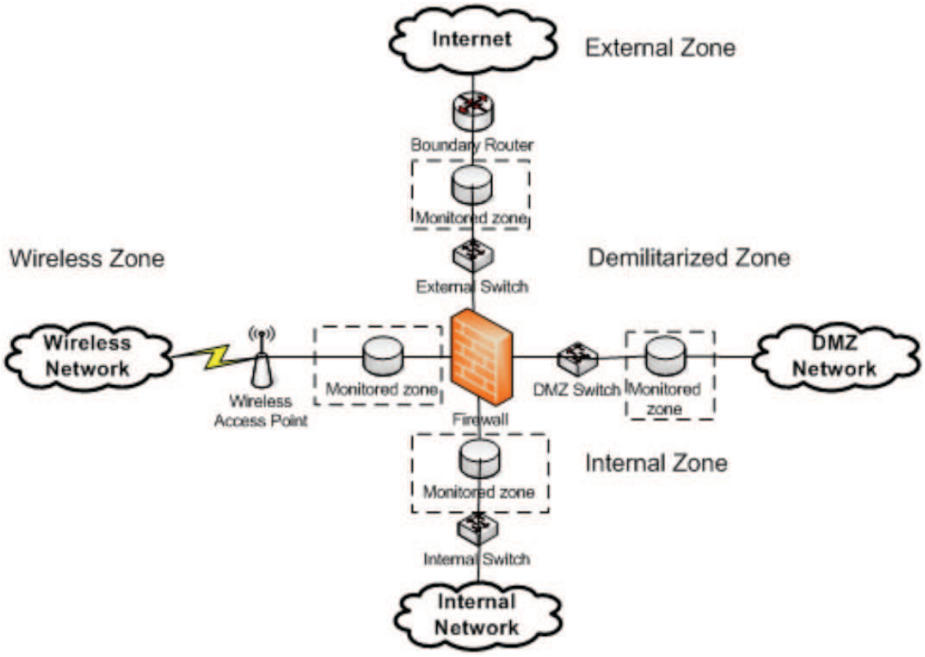


Fig. 4. Enterprise network zoning with monitored zone

This idea has the objective to not being the target that can attack easily and from the attacking. It also and limit the damage when there is an attack. Therefore, these are 5 class of the attacker, the outside attacker that intruding via the Internet (class 1), the outside attacker who intrude via wireless segment (class 2), the internal attacker who intrude via the wired LAN (class 3), and the internal attacker that intrude via the wireless segment (class 4).
This network consists of 4 monitoring zone, installing at the area that there is the inbound and outbound access of traffic, by using firewall as the tool to separate the network into 4 zones in the physical level featured with;
External network zone composed of the external firewall interface through the boundary router, and to the Internet. Internal network zone composed of the internal firewall interface, including every host that is connected until reach the internal switch.
Wireless zone composed of devices and hosts that connect to the wireless. DMZ composed of firewall DMZ interface, including every host that is connected with DMZ switch. The separation of the network into zones will support good security framework, specifying about the rule and security policy that conform with the traffic from each zone clearly and concisely. This make the system can clearly monitor and detect the intrusion.

3.4 Backup and recovery mechanism

To ensure that the survival system, in case of the agent that is one of the components of this architecture stops its process, which might because the lost while transmitting, being attacked, or fail to communicate with other agents in the proper time limit. It will suddenly resume perfectly, do not make others process in IDS being destroyed. This is because we design the rapid backup and recovery mechanism, it is the major part of this architecture because it is the protection using the agent system, and every agent will has more than 1 agent backup as shown in Fig. 5.

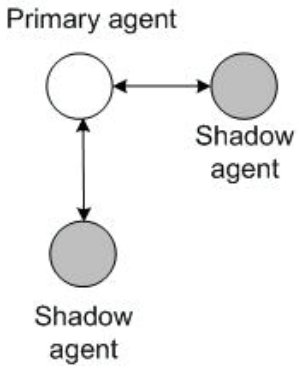


Fig. 5. Agent Backup

Backup agent will keeps all the information or some part of the agent that it is backup as shown in Fig. 6. The recovery process will (1) operational agent with 2 backup agents (2). When the original agent is corrupts. (3) Both backup agents will make a deal to choose the selected the successor. (4) When the successor is selected, it will create the new backup (5), agent that is broken discovers their ability, but the original agent will be terminated.

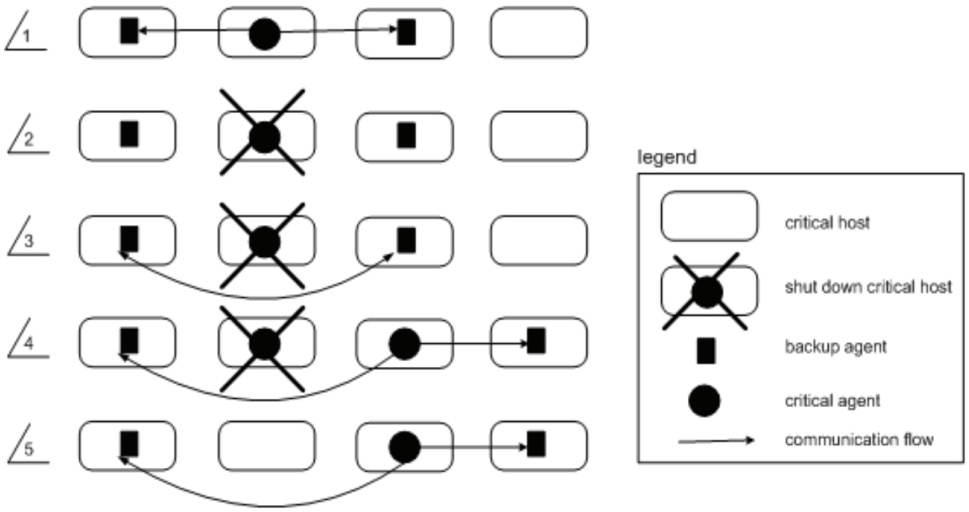


Fig. 6. Backup and recovery mechanism

3.5 Security techniques

To ensure the correctness of the message integrity, we make all of the communications in the components pass only the secured channel, by using the Public-key cryptography that is the Asymmetric scheme encryption and prevent the information by using HMAC (Hashed Message Authentication Code), which is the one component of the Digital signature. We do not need to encrypt overall document, but encrypt only with hash-value that received from the original document for the more execution speed and reduces the density of the transmission on the network.

Moreover, the communication between the groups of the major components will force to communicate via the secure transmission channel, using the VPN (Virtual private network) technique. To reduce network congress ion, we design all communication between components using asymmetric multicasting group.

4. Architecture analysis

For considering whether our designed architecture can be survived or not, we will consider.

4.1 Phase of compromise analysis

If we want to detect the intrusion, we need to understand the actions to make the victim compromised from scanning, infiltrating, until the ability to control over the victim. There are 5 phases [17] to compromise a target, including (1) reconnaissance, (2) exploitation, (3) reinforcement, (4) consolidation, and (5) pillage. Reconnaissance is the process to detect the connection and the number of hosts, the number and type of services, and examine the vulnerability of the application. Exploitation is the process that using those vulnerabilities in the wrong way, changing, or make the victim's service unusable.

Reinforcement is the step of trying to make strength of the intruder, by using the ability of it while infiltrating on the victim. Consolidation is the step that occur when the intruder

communicate to the server of the victim via the Back door and use the victim as the base to intercept the traffic of the communication between the server and the other host. Pillage is the last step of the aim of the intruder; this may be stealing important data, attack the victim, or command to attack other system that is identified, using the victim as the base for attacking, terminating the process, destroying the resource, or spoil the target's whole organization reputation. After understand the procedure and the activities of the attacking, we can design the intruder detection system to handle, detect, analyze, and response to the intrusion easily.

4.2 Attack pattern analysis

From the previous section, we can conclude the attacking pattern from the attacking model into 4 patterns, that are the external attacker that intruding through the Internet (class 1), the external attacker that intruding through the wireless network (class 2), the internal attacker that intruding through the wired LAN (class 3), and the internal attacker that intruding through the wireless network (class 4). Therefore, we can divide the intruder into two groups, the first group is the external intruder that intruding through the Internet and the wireless network, the second group is the internal intruder through the organization network and the wireless network, both group have the bad objective to the organization's resources. However, with the architecture we designed in this research. Although we can see the channel (that comes from which route), the direction (of the attacking), and the intruder type (who, internal or external), but we cannot close these channels for forbid the intruder, because the usual user also use them. It is impossible that the organization do not allow their officers use the internet from the internal hosts. So, we defined the way to access the network for getting to the resources certainly and limited. We divided the network resource into 4 zones, internal network zone, external network zone, wireless zone, and DMZ. Each zone has the certainly controlled in and out path, using firewall to control the flow of the inbound and outbound traffic, defined the 4 zones as the monitored zone and install the monitored host in each zone also. With our proposed architecture, we assume that there is no attacking type, by which channel, and by who can avoid the detecting of our system. Our system can certainly see the intrusion that occurs in any time and any where. Although this assumption does not guarantee that the intrusion detection system will oppose and survive if there is an attack, but we can find the conclusion in the next topic.

4.3 Attack analysis

We defined the attacking type into 4 types, that are (1) penetrate attack, (2) passive sniffing attack, (3) active probing attack, and (4) denial-of-service attack. As considering the sequence of the intrusion in the previous topic, usually the intruder will use type (2) and type (3) for the first phase of the attack to explore the target network, and then in phases 2-5, it will use type (1) and type (2) with the target victim. By considering those 4 attacking types with our designed system architecture, we can analyze the region that the intruder can attack into 3 partitions, which are the region, the proxy partition, and the critical asset partition.

A. Region attacking

Every host in the leaf region can be penetrated. If there hosts can be breaking through, the attacker can certainly use the same pattern to break through other host, for example, the attacker can use the port of the host that is made to listen to the passing packet of the

network that it goes through and enclosing the channel, so every other hosts in the network cannot be use. Moreover, it can use the active probing attack to attack the hosts in other region of the network. If there is the attacker that can break through large amount of hosts without detection, we can conclude that the intrusion detection system is unsafe. We propose the intruder detection system architecture that can continue function and the attacker cannot destroy the critical region that is the main resource of the host. Although the attacker can destroy some segment of the agent that work in this host, the attacker might correct the encoding of the agent for the bad objective. In this case, the backup mechanism for the agent that is in the leaf LAN still can recover the agent back and continue its function.

B. Proxy partition attacking

Although our proposed architecture can hide the important resources of the system invisible for the address and the real IP address by using NAT. This method can protect only Class 1 and Class 2 attacking, but the attacker can know the location of the proxy agent while connecting with the leaf via the region agent. So, the proxy partition can be the target of the attacking. In our architecture, we will change the location of the proxy agent every time after finish each duty with the region agent, but if the attacker that know the location of those agent still can break through those host as in our assumption and if s/he is fast enough, s/he can control that host before the agent get off from the location. In this case, proxy agent that is in the multicast group can be in the danger situation, because the attacker may destroy the agent or waiting in that host to sniff the traffic package of the network. With this method, the attacker will see the address of the shadowed agent; s/he may attack with the fourth method (DoS) on the multicast group until it is failed or attack with the first method to break through the shadowed agent. By the reason that the members of the multicast group are distributed all over the infrastructure of the system, the attack that make the victim failed will not have an effect to all the network and cannot make the group of the left agent stop, and for the first method attacking, the attacker must be fast enough to break through the host that the shadowed agent is exist, because these agents can move its address at any time. The agents will randomly move all over the region, hard to be the still target for probing or penetrating. Under our assumption, the attacker will be detected before it will attack other target.

For the proxy agent partition, the traffic analysis does not help the attacker to find the coordinator agent of the group, because the whole group communicates through the secured channel. So, it is not possible to sniff or analyze the traffic.

For the shadowed agent, our proposed architecture allows to use the public key cryptography for the couple of the agent and the shadowed agent to guarantee the integrity of both of them. In this case, the traffic analysis also cannot be used. In case of both agents do not use the security mechanisms because of wanting to reduce the operating cost or reduce the traffic congestion, it is the cause that the attacker can find the group coordinator and attack that coordinator, making the system failed. However, the shadowed agent of the coordinator can be recovered the process of the system without stopped, and for the segment that do not have the agent, it is not possible to analyze the traffic definitely.

C. Critical asset partition attacking

With the property of survivability of our proposed architecture, it is hard to penetrate the critical section. Because we cannot use the sniffing or probing to get the communicating data between these critical agents and these critical agent is set up not to response other information types than the agreement. The probing of the attacker is not useful, the attacker

may random critical host or uses the critical host's IP address to attack the proxy agent and the shadowed agent simultaneously, after that uses the information to attack the critical host in the future. However, even if the critical agent is attacked, it can recover by using backup and recovery mechanism as presented.
Therefore, we can say that the intrusion detection system in this architecture will not be shutdown whether it is attacked by any attacking pattern. It is truth that if the intrusion detection system cans still function, there is also the ability to detect the intrusion perfectly and countered that intrusion until it can get rid of it. The intrusion detection system in this architecture can recover its process by using backup and recovery mechanism.

5. Analytical result

By analytical result as the previous section, we can found the survival properties of our architecture. The survivability is the idea for continue designing the system that has ability to progress all of the missions, even there is an attack, objection, or situation [17]. The system that has the survivability must have 3 important characteristics that are the resistance, which is the ability to avoid the attack, the recognition, which is the ability to remember the attacking pattern and limit the damage, and the recovery, which is the ability to recover the important services during the attack and recover all the services after the attack.
Using dynamic and sustainable components based on mobile agent technology and conceptual design framework based on fault tolerance model, leads to reduce the problem on single point of failure and emphasis fault tolerant properties.

5.1 Resistance

The designed Survival Architecture for Distributed Intrusion Detection using Mobile Agent has the main characteristics in the durability and avoid the attack by hiding the main components of the system by using proxy agent as the medium in the communication between components, together with using the network topology that separate network resources into zones, make the main components can move around the network by using the mobile agent and use the shadow agent reserved for every agents that have strong reserve mechanism.

5.2 Recognition

Survival Architecture can remember the attacking patterns, because it has the knowledge database that keeps the signature of the intrusion and the system that use the mobile agent can get rid of the damage when it was attacked.

5.3 Recovery

In case of some parts or every part failed, it can recover some of the processes or all of the processes by using the shadow agent together with the fast recovery.

5.4 Single point of failure (SPoF) reduction

The design that moves the Central directory server of all the components to the critical asset and do not allow the communication with other components directly via the Proxy partition will make the Central directory server hind effectively. The single point of failure problem also has been solved.

5.5 Fault avoidance

Avoiding damage is in the form of IDS architectural design. We use this property as a separate architectural design system divided by the critical resources of the network into three sections includes Critical asset, Proxy partition and region. The enterprise network perimeter by zoning to break the trust-host and untrust host separated to the mechanism used to secure appropriate.

5.6 Fault masking

Our design of system architecture and network zoning this property to hide the fault of some of the elements and use the rapid backup and recovery mechanism to work instead.

5.7 Fault tolerance

The architecture, we use several techniques designed to sustain damage, including fault detection, fault location, fault containment and fault recovery. These techniques can all work under the Mobile Agent technology.

6. Proofing

For proofing that our proposed intrusion detection system architecture can be survived.

Theorem:

The architecture of the intrusion detection system using mobile agent that is proposed can be survived.

Proof:

In case of the attacker can attack only the region, proxy partition, and the critical asset partition as in above analysis.
In bad condition, the attacking at the region might be the cause to make the agent at the leaf of the network failed, but can recover rapidly by using the agent in the proxy partition.
In worst case, the intruder may penetrate the region to the agent in the proxy partition, having the possibility to attack the agent in the proxy partition until it is failed. But these agents still can recover by using the shadowed agent.
In worst case, if the attacker can stop the operation of the proxy partition, and may be able to attack the critical agent later. Causing the malfunction in some sections of the critical agent, but those the critical agent still can be recovered by using the recovery mechanism.
In worst case, since it is so little possibility, but if there is the possibility that there is the attacks partly malfunction the intrusion detection system, but those attack cannot destroy all of the intrusion detection system architecture, because we propose the strong and fast backup and recovery mechanism for each section of the architecture.
Therefore, we have proven that the intrusion detection system architecture that is proposed can be survived even if it is attacked.

7. Conclusion, recommendation and future work

7.1 Conclusion

The current research topics about the architecture for Distributed IDS using mobile agent technology is being growth both in approach level and implementation level, but the main

problem of the design that use this concept is dIDS still has some mistakes, especially dIDS has no strength, it cannot deals with the big attack. Our research design the dIDS architecture is robust architecture improvement that is durable and can be survived by using the mobile agent technology with the network topology design, which allocate the resources into 4 separated parts, installs the monitored host onto each of network segment in order to resist the 5 class of the attacker and hides the main resource of the network behind the intrusion detection system. The design avoid the single point of failure, using shadow agent, together with proxy agent, fast backup and recovery mechanism, multicast group and the encryption of the communication between components of IDS. So, our architecture has the survivability that is resistance, recognition and recovery when there is the attacking from the intruder.

Using dynamic and sustainable components based on mobile agent technology and conceptual design framework based on fault tolerance model, leads to reduce the problem on single point of failure and emphasis fault tolerant properties.

7.2 Recommendation

However, our designed architecture, have some main issues that is the interoperability and traffic congestion. Interoperability Because our architecture is the distributed intrusion detection system (dIDS) that is able to detect the distributed intrusion detection system, one of the issue of this system is the limit of the interoperability, in case of working with other distributed intrusion detection systems, especially the real implementation, because the standard of each dIDS are not match with each other. This is the common problem of the researching and developing the distributed intruder detection system.

Traffic congestion

The concept of this designed architecture aim to the strength of the structure, able to handle any intruder, and survived from any pattern of the attack. Therefore, our architecture must be designed for having the secured communication route, using every security technique, by force every communication between components to pass only the secured channel. However, those security techniques will increase the operation cost and also can lead to the traffic congestion in the network.

From this problem, we use HMAC as the security technique for contents integrity, this technique do not need to encrypt all the contents, we will encrypt only hash value that comes from the original for the velocity in the processing and specify to have the asynchronous communication via multicast group for reducing the traffic.

However, for the cryptography that is used in every section of our architecture, we can consider to use Symmetric-key cryptography instead of the Public-key cryptography in some section to reduce the operation cost, having almost the same security standard.

7.3 Future work

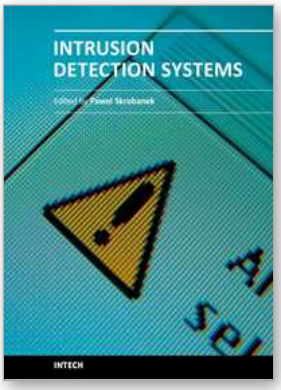
We will work on implementation level using the model to evaluate the performance and proofing the model with survival analysis statistic on the next phase.

8. References

[1] [online]. Available http://www.internetworldstats.com/stats.htm

[2] William Stallings, 2002, Network and Internetwork Security 3th edition, Prentice Hall.

[3] [online]. Available http://staff.washington.edu/dittrich/misc/ddos/
[4] CERT Householder et al., October 2001, Managing the Threat of Denial-of-Service Attacks. [online]. Available http://www.cert.org/archive/pdf/Managing_DoS.pdf
[5] Mukherjee et al., Network intrusion detection, IEEE Network, 8(3):26-41, May/June 1994.
[6] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford and Diego Zamboni, An Architecture for Intrusion Detection using Autonomous Agents, COAST Technical Report 98/05, Purdue University, 1998.
[7] Perter Mell, Donald Marks and Mark McLarnon, A denial-of-service resistant intrusion detection architecture, Computer Network, Special Issue on Intrusion Detection, Elsevier Science BV, 2000.
[8] Kruegel et al., Applying Mobile Agent technology to Intrusion Detection. Distributed Systems Group, Technical University of Vienna, 2002
[9] Tieyan Li, Wai-Meng Chew and Kwok-Yan Lam, Defending Against Distributed Denial of Service Attacks using Resistant Mobile Agent Architecture. In Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'02), IEEE, 2002.
[10] Chunsheng Li, Qingfeng Song and Chengqi Zhang, MA-IDS Architecture for Distributed Intrusion Detection using Mobile Agents. In Proceedings of the 2nd International Conference on Information Technology for Applications (ICITA2004), IEEE, 2004.
[11] Sartid Vongpradhip and Wichet Plaimart, Survival Architecture for Distributed Intrusion Detection System (dIDS) using Mobile Agent. In Proceedings of Sixth IEEE International Symposium on Network Computing and Applications (NCA2007), IEEE, USA, 2007.
[12] P.C.Chan and V.K.Wei, "Preemptive distributed intrusion detection using mobile agents", in Proceedings of Eleventh IEEE International Workshops on Enable Technologies: Infrastructure for Collaborative Enterprises, Jun, 2002.
[13] E. Amoroso and R. Kwapniewski, A selection criteria for intrusion detection systems, in Proceedings of 14th Annual Computer Security Applications Conference, Phoenix, USA, Dec 1998.
[14] A. Birch, Technical evaluation of rapid deployment and re-deployable intrusion detection systems, in Proceedings of IEEE, 1992, International Carnahan Conference on Security Technology, Atlanta, USA, 1992.
[15] Survivable Network, Technology Team, Technical Report, Survivable Network Systems, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-97-TR-013, ESC-TR-97-013, November 1997.
[16] Richard Bejtlich, The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley, 2005.
[17] Pankaj Jalote (1994) Fault tolerance in distributed systems. Prentice-Hall, USA.
[18] George Coulouris, Jean Dollimore And Tim Kindberg, (2001). Distributed Systems, Concept and Design, third edition, Addison-Wesley.



Intrusion Detection Systems

Edited by Dr. Pawel Skrobanek

ISBN 978-953-307-167-1
Hard cover, 324 pages
Publisher InTech
Published online 22, March, 2011
Published in print edition March, 2011

The current structure of the chapters reflects the key aspects discussed in the papers but the papers themselves contain more additional interesting information: examples of a practical application and results obtained for existing networks as well as results of experiments confirming efficacy of a synergistic analysis of anomaly detection and signature detection, and application of interesting solutions, such as an analysis of the anomalies of user behaviors and many others.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Sartid Vongpradhip and Wichet Plaimart (2011). A Sustainable Component of Intrusion Detection System using Survival Architecture on Mobile Agent, Intrusion Detection Systems, Dr. Pawel Skrobanek (Ed.), ISBN: 978-953-307-167-1, InTech, Available from: http://www.intechopen.com/books/intrusion-detection-systems/a-sustainable-component-of-intrusion-detection-system-using-survival-architecture-on-mobile-agent

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821