CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1. Overview

In this chapter, the researcher discusses SAAIDS solution for existing systems, advantages of SAAIDS, system limitation and suggestions for future enhancement. Finally, the achieved objectives and final conclusion are discussed.

7.2. Objective Achieved

The objectives of this research are successfully achieved based on:

a. Objective 1: To design new agent-based IDS based on new architecture in overcoming single-point of failure, delay on information sending and multilevel authorization problem in existing agent-based IDS.

   Based on overall system testing results in Chapter 5, SAAIDS is running as required in system requirements which have been determined in Chapter 3. Single point of failure, delay on information sending and multilevel authorization problem is successfully avoided using the proposed SAAIDS architecture. As mentioned in system testing, agent communication is running

in acceptable time consumption which there are no single point processor existed in the new architecture. All agents in the system have their own components and doing their tasks successfully. Moreover, delay in message sending is not an issue because of the communication between agents using P2P connection which means there are no obstacles can delay the message sending process. All agent has their own administrator which are graded with similar level if authorization for each agent. Therefore, no multilevel authorization problem will exists in SAAIDS architecture. A paper titled The Architecture of SAAIDS has been published in Proceedings of the Fourth IASTED International Conference on Advances in Computer Science and Technology (ACST 2008).

b. Objective 2: To make in-depth study and design new agent communication protocol and algorithm using Elgamal Encryption Algorithm to ensure that communication between agents is secured.

The proposed Agent Communication Protocol and Algorithm has been discussed in Chapter 3 and developed using Elgamal encryption algorithm through specific requirements. Based on system testing on Agent Communication Protocol in agent communication module, the process of agent communication run successfully as required in Agent Communication Protocol's requirements. The message sent securely using the protocol and algorithm.

c. Objective 3: To make in-depth study and design new agent verification protocol and algorithm using Elgamal Digital Signature Algorithm to detect the presence of fake or unauthorized agent which is running in the system..

The proposed Agent Verification Protocol and Algorithm has been discussed in Chapter 3 and developed using SHA1 with Elgamal digital signature algorithm through specific security requirements. Based on the system testing on Agent Verification Protocol in agent verification module, the process of agent verification run successfully as required in Agent Verification Protocol's requirements which needs the protocol to detect fake agent running in the system in specific periodical time. In other hand, the verifier agent is running

on random basis to avoid predictable sequence process in doing agent verification. The test result shown that unauthorized agent detected in the system and a further action was taken immediately in specific reasonable period. A paper titled Agent Verification Protocol in Agent-Based IDS has been published in Proceedings of 8th IEEE International Conference on Computer and Information Technology Workshops (CIT 2008).

7.3. Solution for Existing System

Based on analysis made to three existing systems; AAFID (Autonomous Agent For Intrusion Detection), PAID (Probabilistic Agent-Based Intrusion Detection System) and IDA (Intrusion Detection Agent System) in Chapter 2, few weaknesses or problems of these systems which stated as the problem statements along with their solutions have been identified as below:

a. Architecture of existing agent-based IDS leads to single-point of failure, delay on information sending and multilevel authorization problem.

   In section 3.5.2.1 the researcher discussed about Peer-to-peer (P2P) connection which has been one of agent communication protocol requirement as connection method. As mentioned in the discussion, P2P connection solves all the problems on existing architecture of existing agent-based IDS. The proposed SAAIDS architecture in Chapter 3 which included all components of the system in an agent tends to enable P2P connection between agents. Using P2P connection, single point of failure is avoided because each agent is already doing the monitor or transceiver roles which means no monitor or transceiver between agents in the structure of SAAIDS. Moreover, SAAIDS is fully distributed in structure which means monitoring and detection is done using an agent-based approach, where response decisions are made at the point of analysis. Therefore there is no need for monitor and transceiver to be located outside of an agent. The direct connection also applied in solving delay of information sending because there is no obstacle between agents may able to interrupt or try to delay message sending. Because of only similar agents

existed in the system, the authorization is only in one level which is only for administrator. So, the authorization problems in multilevel structure are avoided. The result of overall testing in Chapter 5 proved that the architecture of SAAIDS is able to avoid all the problems mentioned before.

b. There are many kinds of threats and attacks against agent communication.
In section 3.5, the proposed Agent Communication Protocol and Algorithm has been discussed including its protocol requirements which contains secured communication. The protocol used Elgamal encryption as encryption method to ensure that all message sending in SAAIDS is secured. The result of testing on this protocol in agent communication module in Chapter 5 proved that this protocol provides secure connection between agents in avoiding threats and attacks against agent communication in SAAIDS.

c. There is a threat against agents when an agent has been duplicated which can be exploited to be an unauthorized agent running and doing damages in the system.
In section 3.6, the proposed Agent Verification Protocol and Algorithm has been discussed including its protocol requirements. All the requirements tends to ensure that detection of unauthorized agents process running smoothly as required. The protocol used SHA1 with Elgamal Digital Signature to verify that all agents in the system are authorized agents. The result of testing on this protocol in agent verification module in Chapter 5 proved that this protocol able to detect unauthorized agent in the system and ensuring that all agents in the system are authorized agents.

7.4. The Advantages of SAAIDS

Advantages of SAAIDS have been identified as below:

a. SAAIDS architecture able to avoid single point of failure, delay in message sending and multilevel authorization problems.

b. SAAIDS enhances agent communication security and provides secured channel for agent to send messages.
c. SAAIDS improves agent's protection and ensure agent security by verifying all agents and detecting unauthorized agent running in the system.
d. SAAIDS is an autonomous system which means that not need human intervention after the installation process.
e. Monitor module provides Graphical User Interface (GUI) for system administrator with ability to manually control agents in the system for any kind of event required administrator to do so.
f. Monitor module provides Graphical User Interface (GUI) for system administrator with ability to view detection and verification log for their reference of system's current condition and future enhancement.
g. The administrator login interface completed with authentication process using SHA1 hash algorithm.
h. Authorization information consumes only small size of storage for each agent.
i. Deployment of SAAIDS is efficient because only agents have to be deployed throughout the system same as deploying new agent in the system.

7.5. System Limitation

System limitations are detected in the final development phase of this system which is:

a. The capability of intrusion detection in SAAIDS is limited to update Snort's references at recent time.
b. Agent Communication Protocol used Elgamal encryption as encryption method which an issues has been raised about big key size in Elgamal encryption which may consumes system's memory and effects arriving time of the message sending. This limitation effects on Agent Verification Protocol too due to the same big key size issue.

7.6. Future Enhancement

SAAIDS can be enhanced based on the system limitation. Several enhancements suggested improving this system in the future. The suggestions are:

a. Intrusion detection in SAAIDS can be improved by doing research and development in detecting new type of attacks using other data analysis approaches such as expert system and fuzzy logic.
b. Agent Communication Protocol can be enhanced by using improved encryption method which may shorten time and memory consumption in doing encryption and decryption process such as RSA.
c. Agent Verification Digital Signature can be enhanced using improved digital signature algorithm which may shorten time and memory consumption in signing process such as Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA).
d. The authentication process for administrator can be improved by using improved hash function for password verification.
e. Administrator module can be enhanced with the ability to simulate the condition and status of agent communication and agent verification processes occurred in SAAIDS.

7.7. Conclusion

The research and development of SAAIDS is begun with in-depth study and research on intrusion detection and IDS. In developing the architecture of SAAIDS, many related works was studied and reviewed in determining issues and problems on the existing agent-based IDS. All the weaknesses gathered and several main problems had been determined as mentioned in problem statements. The objectives of this research project have been determined with all projects' statements in Chapter 1 as well as research methodology.

Then, all needed information gathered through literature reviews in getting better understanding of attacks, intrusion detection and IDS and cryptography in IDS. After that, issues and problems determined given further discussion followed by proposed solution in Chapter 2. The issues and problems discussed based on the raised weaknesses in existing agent-based IDS which are single-point of failure, delay in information sending and multilevel authorization problem and followed by network attacks against agent communication. Finally, duplication of agents problem discussed in this chapter.

Chapter 3 discussed system development methodology which are Prototype model as process model of system development and Unified Modeling Language (UML) as tool for system design methodology. All the design diagrams required in UML are discussed which containing design diagrams for each protocol and module involving use case diagram, activity diagram, sequence diagram, package diagram, class diagram and database diagram had been designed. The related Graphical User Interface (GUI) for certain modules are shown in this chapter.

The system architecture and design is described in details in Chapter 4 which begins with requirement acquisition and determination. The first proposed solution which is the architecture of SAAIDS. The proposed architecture successfully determined and contained all components required in IDS which included in an agent. P2P connection used as connection method in agent communication. The architecture of SAAIDS which built as an agent and P2P connection developed to solve problems in existing architecture in agent-based IDS. The proposed Agent Communication Protocol and Algorithm is developed to solve the second problem. The protocol used to provide secured agent communication from attacks. Then, the duplication of agent problem is catered by Agent Verification Protocol and Algorithm which detecting unauthorized agent in system.

Information filter and data analysis in Detection module used Snort as the processor. Detection response process is done through Detection Response in Monitor module. Meanwhile, the Verification response from agent verification process sent to Verification Response in Monitor. Both of the responses are broadcasted to all agents

to ensure that AgentDB and DetectionDB in each agents in the system are up-to-date. Administrator in Monitor module provides two facilities for administrator which is logs viewing and agent controlling. The administrator has to be verified to log into the system through a login interface to ensure that only authorized administrator can logs into the system. The login interface completed with authentication process using SHA1 hash algorithm and the record of every administrator stored in AgentDB.

The system implementation is discussed in Chapter 5 which contains the proposed architecture's components which designed to be modules for implementation phase. Agent Communication and Agent Verification algorithms are developed to be implemented. Related Graphical User Interface (GUI) and coding with explanation of the proposed modules and algorithms are shown and further discussed.

Testing of related modules of the system is discussed in Chapter 6. Each of the coding are tested through white-box and black-box testing. The architecture, agent communication and agent verification protocols are tested with different factors which are validity and reliability testing. All the test result produced proved that SAAIDS is successfully developed.

The contributions of this research are represented by the new designed of architecture of SAAIDS, enhancement of agent communication security in agent-based IDS with development of Agent Communication Protocol and Algorithm and detecting unauthorized agent with the new designed of Agent Verification Protocol and Algorithm. The ideas of agent verification process is raised from issues reviewed that emphasizes on agent duplication and system protection From researcher's reviews, there are no such protocol existed in existing agent-based IDS and being a main contribution of this research project.

It is a hope; this research can be used as guidance to administrators and other researchers in improving and enhancing the technology of IDS. The system limitation and suggested future enhancement stated above may be sources of ideas inspiration of researchers and administrator to gain knowledge and do more research about IDS in

enhancing existing agent-based IDS and moreover, developing new technology of agent-based IDS.