CHAPTER 1

INTRODUCTION

1.1. Project Definition

Due to the increasing usage of Internet and its huge ability and availability, confidentiality always seems to be threatened. In addition with increasing number of services and business activities which are running through internet and intranet connectivity, the usage of online payment and information transfer are borderless. This so-called borderless world has a major drawback which is security.

Most people keep a lot of valuable information on their personal computers, such as financial records and electronic diaries that they do not want to share with others. However, many fail to realize that when the computers are hooked to the Internet, actually they are allowing unauthorized personal to trespass into their personal computers. Here, anyone with little know-how can try and break in and have a look around. The situation is more serious for organizations that are dealing with confidential data such financial institutions, military and national registration records.

According to Infonetics Research's latest Network Security Appliances and Software report, worldwide network security appliance and software sales are forecast to pass the $5 billion mark for the first time in 2007(Wilson, 2007). Network Security

Appliances and Software represents integrated security appliances in six prices categories, secure routers, SSL VPN gateways, VPN and firewall software, and host and network-based intrusion detection system (IDS) and intrusion prevention system (IPS) products. This research produced an essential report shows that network security has been a big business nowadays. Actually, his situation is an implication from increasing of unstoppable cyber crimes series occurred every day. Dealing with computer-related and cyber crimes, in 2007, CSI/FBI released its 2007 report (Computer Security Institute, 2007) with news that the average annual loss reported by United State companies in the 2007 CSI Computer Crime and Security Survey more than doubled, from $168,000 in last year 2007 report to $350,424 in year 2008 survey. This survey shows that cyber crimes has been highlighted and caused big financial loss to the government and companies in United States. In Malaysia, incidents statistic produced by MyCERT/CyberSecurity for year 2006 shows that total of 1038 incidents of network attacks occurred and more than 37% (385 incidents) of them came from intrusion (MyCERT/CyberSecurity, 2007). This incident statistic shows that intrusion detection is a major problem among other incidents in Malaysia which reported by organizations and public member.

Beginning in 1980, based on James Anderson's paper in Computer Security Threat Monitoring and Surveillance, the notion of intrusion detection was born (Innella, 2001). Since then, several pivotal events in IDS technology have advanced intrusion detection to its current state. Agent-based IDS is one of famous IDS technologies for time being. Autonomous Agents for Intrusion Detection (AAFID) is a project under Center for Education and Research in Information Assurance and Security (CERIAS) established on 1998 when the first public release produced (Balasubramaniyan et al., 1998). Intrusion Detection Agent System (IDA) project was initiated in 2001 by Information-technology Promotion Agency (IPA) based on network intrusion detection in solving conventional IDS lack and introducing more intrusions-related mechanism more than user's activities (Asaka M. et al., 2001). The progress of agent-based IDS is tremendous since then many research related was done because of its advantages, such as overcoming network latency, system scalability, reduce network load and platform independence (Albag, 2005).

The main aims of this project are to make in depth study about IDS and to emphasize on agent communication and verification, followed by designing their protocols and algorithms in agent-based IDS. These protocols and algorithms are completed with security mechanism, towards guaranteeing the reliability of the system.

This research targets to give guidance to IT personal, security analyst and network administrator in their works and studies towards performing better intrusion detection in the future.

1.2. Problem Statements

There are a number of issues and problems in intrusion detection. Classification of intrusion detection is an essential aspect to be acknowledged to ensure deep understanding about intrusion detection. Some of the problems lead to security issues of the system itself (Douglas J.B. et al., 2001). Please refer section 2.3 and 2.8 for further explanation. From research's observation and study, these are the identified problems:

a. The existing architecture of agent-based IDS leads to single-point of failure, delay on information sending and multilevel authorization problem.
b. There are many network attacks against agent communication.
c. Duplication of agents which leads to exploitation by fake or unauthorized agent caused damages in the system.

1.3. Project Motivation

Based on researcher's research and observation, there are several motivations that encouraged in doing this project. Firstly, in Malaysia, there are very limited numbers of study carried out on intrusion detection compared to the large number of intrusion incidents have been reported every year (MyCERT/CyberSecurity, 2007). This study can be used as guidance in handling intrusion incidents especially in Malaysia.

Secondly, there are limited numbers of study that emphasize on agents' security specifically agents that involve in communication and verification processes. This study made an in-depth exploration on both area and it can be used to help researchers and organizations towards providing better IDS in the future.

1.4. Project Objectives

Based on the problem statement in section 1.2, the objectives of this project are:

a. 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.
b. 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.
c. 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.

1.5. Research Questions

In order to achieve the objectives defined above, the research questions identified are:

a. What are components needed in designing new architecture as a basis of agent-based IDS in overcoming single-point of failure, delay on information sending and multilevel authorization problem in existing agent-based IDS?
b. What are security mechanisms have to be identified to design agent communication protocol and algorithm in order to ensure that communication between agents is secured?

c. What are security mechanisms have to be identified towards to design agent verification protocol and algorithm in order to detect the presence of fake or unauthorized agent which is running in the system?

1.6. Research Methodology

In achieving the objectives above, this section outlines research methodology used. This methodology combined 12 phases which has been done continuously. Figure 1.1 shows the flowchart of research activities. The phases are:

a. Doing Preliminary Research

Preliminary research is including discussions titled Threats, Attacks And Intrusions, Attacks Classification In SAAIDS, Recovering From Intrusion, Intrusion Detection System, Data Analysis Approaches, Cryptology In Intrusion Detection System, Related Works, Issues And Problems In Previous Works and Proposed Solution

b. Designing SAAIDS architecture

This phase focuses on designing SAAIDS architecture in overcoming the issues and problems raised in agent-based IDS.

c. Designing of an autonomous agent

An agent is designed based on SAAIDS architecture.

d. Testing an autonomous agent

The agent designed before is tested for intrusion detection using specific testing methodology. Mimic attacks will be used to evaluate this agent.

e. Designing multiple autonomous agents

The single agent is duplicated including all intrusion detection tasks to make agent communication and verification available.

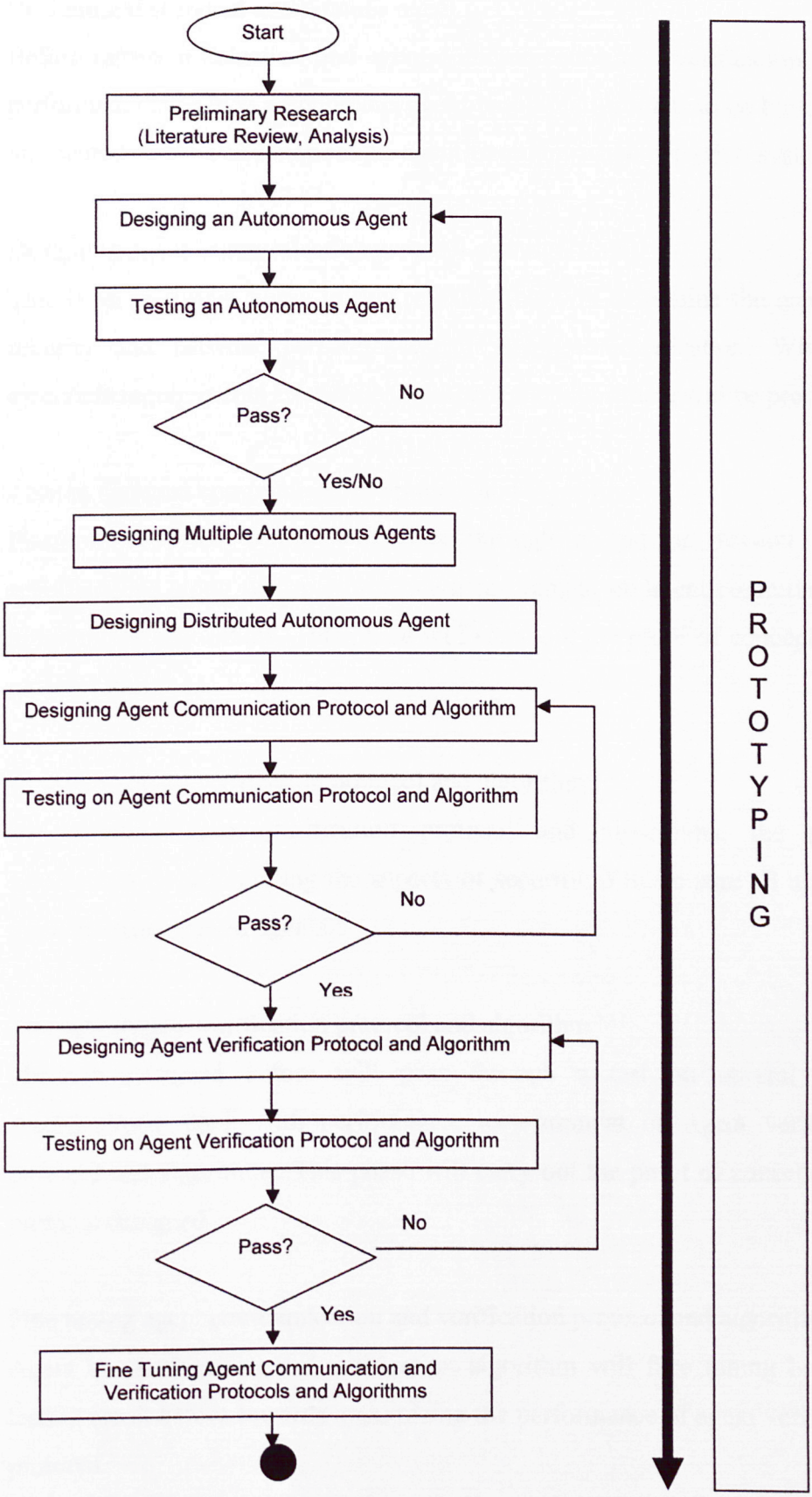

Figure 1.1: Research Activity Flowchart

f. Designing distributed autonomous agent

Before intrusion detection and agent communication and verification can be performed, distributed autonomous agent-based platform has to be build based on secured distributed autonomous agent-based intrusion detection system.

g. Designing agent communication protocol and algorithm

This is an important phase in this research that will determine the aspects of security and network performances of agent communication. When the essentials requirements are defined, protocol and algorithms will be produced.

h. Testing on agent communication protocol and algorithm

Platform designed before will pass through a test on several testing specifications along with performance measurement on agent communication protocol and algorithms. This phase will carry out the proof of concept of the protocol designed.

i. Designing agent verification protocol and algorithm

In designing agent verification protocol and algorithms, the process emphasizes on determining the aspects of security to make sure all agents in the system are trusted agents.

j. Testing on agent verification protocol and algorithm

Platform designed before will pass through a test on several testing specifications along with performance measurement on agent verification protocol and algorithms. This phase will carry out the proof of concept of the protocol designed.

k. Fine tuning agent communication and verification protocol and algorithms

Agent communication and verification algorithm will face tuning based on testing result before towards maximizing the performance of agent verification protocol.

l. Technology dissemination

The final part of this research is technology dissemination where the protocol and algorithms designed along with test result will be presented in international conference and technology exhibition. Patent and commercialisation will be the final step of this phase.

1.7. Project Scope

In designing agent-based IDS, only three agents are developed along with each agent performs its different detection approach based on packet analysis. Since this project tends to emphasize on developing secured system architecture, agent communication and agent verification protocol and algorithm, researcher assumes that this system is already equipped with Snort as intrusion detection tool to do packet filtering and intrusion detection to ensure the objectives of this project achieved. Then, this project emphasizes on developing agent communication and verification protocol and algorithm followed by monitoring system used by administrator to perform log monitoring. Existing cryptography technologies in authentication, encryption and digital signature such as SHA1, Elgamal encryption and digital signature used in this system in developing agent communication and agent verification protocol and algorithm. However, this project is more concern in detecting the presence of fake or unauthorized agent. Besides that, testing phase for this system uses resources from several organizations such as virus definition or attack/intrusion library. Testing and evaluation phase only be performed on the three agents using agent communication and agent verification protocol and algorithm based on testing environment which is held on private network connection.

1.8. Project Limitations

The monitoring system produced for this research developed using Java because of its reliability of outcomes in performing on multiplatform. Testing and evaluation phase

uses attack samples from existing researches or organizations and performed on a small area of network as evaluation environment which mimics the real environment.

1.9. Target Audiences

The target audiences are IT personal, security analyst and network administrator.

1.10. Project Expected Outcomes

The project expected outcomes are:

a. To produce a new design of agent-based intrusion detection system called Secured Autonomous Agent-based Intrusion Detection System (SAAIDS).
b. To produce a design of new agent communication protocol and its algorithm to detect attack or threat against communication between agents.
c. To produce a design of new agent verification protocol and its algorithm to detect the violation of fake or unauthorized agent which is running in the system.

1.11. Terminology

Below are terms and its definition and description used throughout the project that perhaps can be helpful towards further understanding prior reading this research paper:

a. Intrusion Detection

   Intrusion detection is a process of monitoring events occurring in a computer system or network and analyzing them for signs of *intrusions,* defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network (Bace & Mell, 2001).

b. Autonomous Agents

Autonomous Agents are a group of free-running processes which can act independently of each other and the system (Heady, 1990).

c. Fully Distributed Agents

Fully Distributed Agents is a structure or control strategy of IDS. Monitoring and detection process is done using agent-based approach, where response decisions are made at the point of analysis (Bace and Mell, 2001).

d. Attack Event

Attack Event is defined as a scenario when an attack or intrusion occurred in a system.

e. Detection Approach

Detection Approach in intrusion detection is defined as a technique of detection which involving two main techniques; anomaly detection and signature detection (Kazienko and Dorosz, 2004).

f. Data Analysis

Data Analysis is a process of analyzing data and decision-making either an intrusion occurred or not.

g. Analysis Timing

Analysis Timing is defined how and when data analysis process runs in IDS consisting two major categories; real-time-based and interval-based (Kazienko and Dorosz, 2004).

h. Response

Response is defined as an action after an intrusion occurred in IDS which involving two types; active or passive (Kazienko and Dorosz, 2004).

i. Agent Communication

Agent Communication is a term used to brief how agent communicates each other including its security mechanism.

j. Agent Verification

Agent Verification is a term used to explain how to make sure each agent in the system is a trusted agent through its security mechanism.

1.12. Project Schedule

Project schedule for this project is shown in Gantt chart format as per attached at Appendix A.

1.13. Organization of Project Report

This project is organized into six related chapters. Chapter 1 is Introduction which presents the introduction of this project. It starts by presenting the project definition, problem statements, project motivation, project objectives, research question, research methodology, project scope, project limitations, target audiences; project expected outcomes, terminology, project schedule and organization of this project report. The last section is the conclusion of this project.

Chapter 2 is Literature Review which provides literature reviews done for this project starting with overview of this chapter. Then followed by discussion on following topics; Threats, Attacks and Intrusion, Attacks Classification in SAAIDS, Recovering From Intrusion, Intrusion Detection System, Data Analysis Approaches, Cryptology In Intrusion Detection System, Related Works, Issues And Problems In Previous Works And Proposed Solution. This chapter ends with conclusion.

Chapter 3 is System Methodology which discusses methodology used for system development and design which are involving system requirements analysis, system analysis, system design and database design.

Chapter 4 is System Architecture and Design which presents the architecture of SAAIDS and discusses about the requirements and processes of intrusion detection, agent security, agent communication protocol and algorithm and agent verification protocol and algorithm.

Chapter 5 is System Implementation which represents the design of every module in the system module design. In this chapter, coding for each module in this system and interfaces that related with the coding is being discussed in details.

Chapter 6 is System Testing which contains testing approaches applied to test the communication between agents is secured and to detect the presence of fake or unauthorized agent which is running in the system.

Chapter 7 is Conclusion and Future Works is the final chapter which contains solution for existing system, advantages of SAAIDS and system limitation. Finally, suggestion for future enhancement and objective achieved are discussed at the end this project report.

1.14. Conclusions

There is great need to produce more researches and studies about intrusion detection in considering large number of intrusion incidents occurred all over the world. In-depth study has to be carried out in overcoming intrusion detection issues and problems. The security and issues are very important factors to be solved to guarantee the reliability of the system itself. This research defines new classification on IDS and agent-based IDS. Besides that, this research focused on agent communication and agent verification in overcoming the issues above-mentioned.