On an IT Security Framework

Dharmendra Sharma, Wanli Ma, and Dat Tran

School of Information Sciences and Engineering
University of Canberra, ACT 2601, Australia
{Dharmendra.Sharma,Wanli.Ma,Dat.Tran}@canberra.edu.au

Abstract. IT security is becoming an area of increasing importance especially with the increasing dependency of humans and businesses on computers and computer networks. This paper outlines a generic framework to deal with security issues. The framework proposed is based on a multi agent architecture. Each specialist task for security requirement is modeled as a specialist agent task and to address the global security tasks an environment is invoked in which the multiple agents execute their specialist skills and communicate to produce the desired behavior. This paper presents the framework and its constituent parts and discusses the characteristics of the security problems, the agent roles and how they link up. The security related areas investigated in the current study are discussed and modeled in the proposed framework.

1 Introduction

Nowadays, computers pervade every aspect of human life, ranging from personal entertainment, office operation, corporate business, finance hubs, such as banking and stock exchange systems, and critical infrastructure control to defense and weaponry systems. These computers are connected through wired or wireless connection to generate networks for resource sharing through which processing power or typically large amounts of data are exchanged.

The management of the computers, network devices, and other IT equipment is increasing in complexity with time. The development and implementation of computer systems far out pace computer security needs. Many of the systems currently in place are running critical business, yet little research and development work have been done to secure these systems. Recent trends show a sharp increase in computer security breaches [1] and incidences of virus and worm attacks [2]. The costs incurred in dealing with these security problems are phenomenal. In 2004, in Australia, on average, IT crime and IT security related incidents cost $116,212 per organization [1], while the potential of damage would be even bigger if we take the loss of productivity, loss of confidence in IT, and the resulting negative impact on business.

Despite these difficulties, we are not in a position to readily answer questions such as "*What defenses do I have that will be effective against this attack?*" or "*How do I prevent such attacks in the future?*" [3]. Much work needs to be done to develop security technology and market them to gain user confidence for their uptake of information technology for their secure needs.

R. Khosla et al. (Eds.): KES 2005, LNAI 3681, pp. 226–232, 2005.

IT security covers many issues such as security policy development and implementation, user education, encryption, system administration, network firewall, intrusion detection, and programming practice etc [4]. To secure an IT infrastructure, which consists of the involved computer systems and network devices, many efforts from different areas should be taken. The IT infrastructure is an integrated entity and so it should have security management.

In this paper, we propose an IT security framework. We attempt to systemically integrate research work in several areas of security: system administration assistance, biometrics authentication, intrusion detection, and computer forensics. The proposed security framework integrates the various tasks of gathering security information, analysis of this information using experiential knowledge, generating alert and actions to respond to any security breaches or attempts on breaches. The functionality is integrated in a multi agent distributed environment.

2 Software Agents

A software agent is "*a software entity which functions continuously and autonomously in a particular environment*" [5]. The continuous and autonomous nature of agents and the communication among these agents make them a primary candidate as the underlying framework for IT security. There are many advantages of using multiple agents:

- **An Agent Has Local Knowledge**
  Any security related operation requires the knowledge of IT devices, such as firmware version; operating system type and version, patched levels, and the role of the devices etc. It is virtually impossible to collect this information in a central repository. The information changes constantly. On the other hand, some of the information is only useful to a local device, for example the virus signature data on a particular computer, open ports and provided services on another computer, and remote access to a network router etc. It makes perfect sense to have this information collected, kept, and used by a local software agent. A software agent thus has the local knowledge. It uses or provides the knowledge when needed.
- **An Agent Can Specialize in One Specific Area**
  An agent can also be specialized in a specific area, for example, an intrusion detection agent, an authentication agent, and a traffic analysis agent etc. We can also have different skilled agents to work on the same task. For a piece of information, we can have agents with different skills to examine if there is any trace of intrusion. An agent may be programmed with pattern-matching skills, another agent may be programmed with neural network skills, yet the third agent may be programmed with Hidden Markov Model. This simulates how humans analyse and solve problems, where the same piece of information maybe analyzed by experts with different skills for different purposes.
- **Survivability**
  Due to the distributed and autonomous nature of agents, an agent system can easily survive the loss of some agents. From a system point of view, a large system consists of my components. These components have certain degree of reliability. Such systems have to detect and deal with the possibility of component failure.