Chapter X
MAITS:
A Multi-Agent-Based IT Security Approach

Dharmendra Sharma
University of Canberra, Australia

Wanli Ma
University of Canberra, Australia

Dat Tran
University of Canberra, Australia

Shuangzhe Liu
University of Canberra, Australia

Mary Anderson
University of Canberra, Australia

ABSTRACT

In this chapter, we propose a multi-agent-based information technology (IT) security approach (MAITS) as a holistic solution to the increasing needs of securing computer systems. Each specialist task for security requirements is modeled as a specialist agent. MAITS has five groups of working agents—administration assistant agents, authentication and authorization agents, system log monitoring agents, intrusion detection agents, and pre-mortem-based computer forensics agents. An assessment center, which is comprised of yet another special group of agents, plays a key role in coordinating the interaction of the other agents. Each agent has an agent engine of an appropriate machine-learning algorithm. The engine enables the agent with learning, reasoning, and decision-making abilities. Each agent also has an agent interface, through which the agent interacts with other agents and also the environment.
INTRODUCTION

Computers pervade every aspect of human life, ranging from personal entertainment to critical defense and weaponry systems. These computers are connected via networks that enable resource sharing through the exchange of processing power or large amounts of data. The development and implementation of computer systems far out pace computer security advancements. Many of the systems currently in place are running critical business, yet little effort has been made to secure these systems. We are not in a position to readily answer questions such as (Saydjari, 2004):

- Am I under attack?
- What is its nature and origin?
- What are the attackers doing?
- What might they do next?
- How does it affect my mission?
- What defences do I have that will be effective against this attack?
- What can I do about it; what are my options?
- How do I choose the best option? or
- How do I prevent such attacks in the future?

A great deal of work needs to be done to develop and market security technologies and to supply users with the confidence they need to employ these technologies for their security needs.

In this chapter, we propose a multi-agent-based IT security approach (MAITS) to solve the increasing needs of securing computer systems in a fast-changing IT security landscape. Each specialist task required for security is modeled as a specialist agent task. To address the global security tasks, an environment is invoked in which multiple agents (a multi-agent system or MAS) execute their specialist skills and then communicate with each other to produce the desired behaviour. The discussion of agent roles is systemically integrated with research conducted in several areas of security: system administration assistance, biometrics authentication, intrusion detection, and computer forensics. The proposed security system combines the various tasks of gathering security information, analysing the information using experiential knowledge, and generating alerts and actions to respond to any security breaches or attempts on breaches. The functionality is implemented in a distributed multi-agent environment.

This chapter commences with a look into the background of information technology (IT) security threats that inspire the need to protect computer systems, the process perpetrators may follow when making an attack, and an introduction into the agent technology that forms the basis for MAITS. This is then followed by a discussion of the current research work in the development of MAITS. The chapter concludes with a summary.

BACKGROUND

In this section, we will first briefly study security threats and agent technology. We will then discuss the motivation for MAITS.

Security Threats

Since 2000, several high-profile computer viruses/worms, such as CodeRed (Code Red, 2001), Slammer (Slammer Virus, 2003), and the LoveBug (Love Letter Worm, 2001), have caused havoc to IT infrastructure, resulting in millions of dollars in damages. According to an AusCERT survey, in 2004 alone, the average cost for IT crime- and IT security-related incidents was $116,212 per organization in Australia (Australian Computer Crime & Security Survey, 2004). On August 14, 2005, a new worm, Zobot, appeared (Zobot Worm, 2005). Zobot went beyond causing damage, indicating a new trend designed for financial gain (Krebs, 2005). Given the new
Related Content

The Performance of Grey System Agent and ANN Agent in Predicting Closing Prices for Online Auctions
[www.igi-global.com/article/performance-grey-system-agent-ann/60653?camid=4v1a](www.igi-global.com/article/performance-grey-system-agent-ann/60653?camid=4v1a)

Fundamentals of Pedestrian and Evacuation Dynamics
[www.igi-global.com/chapter/fundamentals-pedestrian-evacuation-dynamics/26936?camid=4v1a](www.igi-global.com/chapter/fundamentals-pedestrian-evacuation-dynamics/26936?camid=4v1a)

An Agent Based Hydro Informatics Approach for the Engagement of Farmers in Irrigation Water Management in Saudi Arabia

A Collaborative Multi-Agent Framework for Internet-Based Teleoperation Systems
[www.igi-global.com/article/a-collaborative-multi-agent-framework-for-internet-based-teleoperation-systems/87165?camid=4v1a](www.igi-global.com/article/a-collaborative-multi-agent-framework-for-internet-based-teleoperation-systems/87165?camid=4v1a)