Mobile Agent Based Network Defense System in Enterprise Network

Yu Cai, Michigan Technological University, USA

ABSTRACT

Security has become the Achilles’ heel of many organizations in today’s computer-dominated society. In this paper, a configurable intrusion detection and response framework named Mobile Agents based Distributed (MAD) security system was proposed for enterprise network consisting of a large number of mobile and handheld devices. The key idea of MAD is to use autonomous mobile agents as lightweight entities to provide unified interfaces for intrusion detection, intrusion response, information fusion, and dynamic reconfiguration. These lightweight agents can be easily installed and managed on mobile and handheld devices. The MAD framework includes a family of autonomous agents, servers and software modules. An Object-based intrusion modeling language (mLanguage) is proposed to allow easy data sharing and system control. A data fusion engine (mEngine) is used to provide fused results for traffic classification and intrusion identification. To ensure Quality-of-Service (QoS) requirements for end users, adaptive resource allocation scheme is also presented. It is hoped that this project will advance the understanding of complex, interactive, and collaborative distributed systems.

Keywords: Information Fusion, Intrusion Detection, Intrusion Response, Mobile Handheld Devices, Quality-of-Service

INTRODUCTION

Security has become one of the most critical issues in today’s computer-dominated society. Security threats have increased in sophistication, frequency and complexity in the past couple of decades. Despite the continuous efforts from the security community, organizations are being attacked at an alarming rate nowadays. Particularly for large scale enterprise network consisting of a number of mobile and handheld devices, there is a mismatch between the level of protection that current security measures are providing and the level needed to address their actual degree of risks. The characteristics of the mobile and handheld devices make incorporating security very challenge. The constraints on mobile and handheld devices make the design and operation different from the contemporary wired networks. Security has become the Achilles’ heel of networks of all sizes.

The monitoring and surveillance of security threats in network systems are mostly done by Intrusion Detection System (IDS) (Douligeris & Serpanos, 2007). IDS are based on the principle...
that attacks on computer systems and networks will be noticeably different from normal activities. The job of IDS is to detect these abnormal patterns by analyzing information from different sensing sources in the network.

IDSs may be classified into host-based IDSs, network based IDSs and distributed IDSs, according to the source of audit information. Host-based IDSs get data from host audit trails; network-based IDSs collect network traffic as the data source; distributed IDSs gather audit data from multiple hosts and the network. There has been a shift from a centralized and monolithic IDS framework to a distributed one (Balasubramaniyan & Fernandez, 1998). Distributed IDSs usually include multiple sensors or agents for intrusion detection, and information fusion modules for data correlation.

However, when deploying IDSs in enterprise network with a large number of mobile and handheld devices, the IDS systems usually suffer from a number of limitations.

- **Configurability, controllability and manageability.** Today’s networks are dynamic with mobile and handheld devices. IDSs need to support flexible on-demand re-configuration and dynamic deployment of new nodes. For example, tasks like loading attack signatures at run-time, creating new detection sensors, being adaptive to changes in the environment, and detecting new attacks should be supported.

- **Interoperability.** Today’s networks are heterogeneous with mobile devices from different vendors. Many IDSs are developed and operated in specific domains and environments. It is a complicated and error-prone task to integrate and coordinate multiple IDSs. Mechanisms need to be designed to support the effective integration, cooperation and collaboration of heterogeneous IDSs.

- **Scalability, extensibility and robustness.** IDSs should be scalable to monitor large scale networks with limited overhead imposed. IDSs need to be lightweight to run on mobile and handheld devices. IDSs need to protect themselves from attacks. They should also be able to recover quickly from system crashes or network failure.

- **Effectiveness.** IDSs suffer from the problem of high false alarm rate, including false positive and false negative. Algorithms need to be designed to produce real time, high-confidence detection results by fusing information from multiple data sources.

- **Global Coordination.** Network intrusion detection and prevention should utilize both local surveillance and global coordination. Local surveillance secures a protection domain by proactively identifying and thwarting attacks. Global coordination integrates the information from different parts of the network and coordinates collective countermeasures.

Therefore, IDS involving mobile and handheld devices is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to wireless network.

In this paper, we propose a highly-configurable, well-integrated intrusion detection & response framework named Mobile Agents based Distributed (MAD) security system for enterprise network with mobile and handheld devices. The key idea of MAD is to use mobile autonomous agents (hereby referred to as AA) as lightweight, independently-running entities to provide unified interfaces for intrusion detection, intrusion response, information fusion and dynamic reconfiguration. All these AAs are mobile agents which can travel among network hosts and take actions at target spots. The reason of using mobile AA is that they can be sent to security hot spots or blank spots to install new AAs or perform other tasks with great flexibility. Lightweight agents reduce the running overhead on mobile and handheld devices. This feature is designed to fit dynamic nature of enterprise network with mobile and handheld devices.

Multiple AAs are coordinated to obtain a global view of the security state and take collective countermeasures against attacks. AAs are designed to carry out tasks in a flexible, adap-
Related Content

What is New about the Internet Delay Space?
www.igi-global.com/article/what-is-new-about-the-internet-delay-space/144444?camid=4v1a

The Role of B2B E-Commerce in Market Share: Evidence from Spanish Manufacturing Firms
www.igi-global.com/chapter/the-role-of-b2b-e-commerce-in-market-share/183340?camid=4v1a
A Study of Reusing Smartphones to Augment Elementary School Education
[www.igi-global.com/article/study-reusing-smartphones-augment-elementary/67098?camid=4v1a](www.igi-global.com/article/study-reusing-smartphones-augment-elementary/67098?camid=4v1a)

Tools for Rapidly Prototyping Mobile Interactions
[www.igi-global.com/chapter/tools-rapidly-prototyping-mobile-interactions/21840?camid=4v1a](www.igi-global.com/chapter/tools-rapidly-prototyping-mobile-interactions/21840?camid=4v1a)