Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Network and
Computer Applications 28 (2005) 183–208

Journal of NETWORK and COMPUTER APPLICATIONS

www.elsevier.com/locate/jnca

An agent-based approach to security service

Elhadi Shakshuki*, Zhonghai Luo, Jing Gong

Jodrey School of Computer Science, Acadia University, Wolfville, NS, Canada B4P 2R6

Received 20 January 2004; received in revised form 24 June 2004; accepted 25 June 2004

Abstract

The tremendous growth of the network-centred (Internet and Intranet) computing environments requires new architecture for security services. Computer crimes are growing rapidly in these environments. In addition, these computing environments are open, and users may be connected or disconnected at any time. This makes computer security a necessity to all computer users. This paper presents a multi-agent system architecture for security services. The main objective of this system is to address some of the shortcomings that are present in contemporary security service systems that focused on providing solutions for specific security issues, such as authentication and authorization. Another objective is to provide a relatively complete security service solution to protect hosts and users. The proposed system architecture includes four types of agents: interface, authentication, authorization, and service provider agents (SPAs). The interface agents interact with the users to fulfill their interests. The authentication agents investigate the validity of using keystroke dynamics to strengthen security. The authorization agents make all decisions regarding who can access which resources and for what purposes. The SPAs offer different encryption services to different users. This paper provides the agents' architecture, design and implementations that enable them to cooperate, coordinate, and communicate with each other to provide a secure environment. A prototype of the system is implemented using the Java Agent Development Framework.

Keywords: Agent; Security; Multi-agent; Authentication; Authorization

* Corresponding author. Tel.: +1-902-585-1524; fax: +1-902-585-1067.
E-mail address: elhadi.shakshuki@acadiau.ca (E. Shakshuki).

1084-8045/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2004.06.004

1. Introduction

With the wide use of Internet-based applications, security in distributed systems becomes a serious issue to individuals, companies and organizations. This makes computer security a necessity to all computer users. Thus, many users use a security service that can be used to protect them from others. However, security services require extra computing resources because they are time-consuming. The main objective of this work is to develop a multi-agent system that acts as a middleware between the user and the network-centred computing environment. The main design principles of the system are that the system should provide the user with fast, efficient, stable and flexible security service. The agents interact cooperatively in a distributed environment and collectively act on behalf of the users to provide them with a secure environment. This paper presents a multi-agent system architecture that is built to accommodate the design principles. In addition, security is achieved at different levels. At the first level, the user is authenticated. At the second level, the user is authorized. At the third level, the service provides encryption, decryption, digital signature and verification.

The accurate authentication of users is one of the main important issues in distributed information systems. An efficient authentication can accurately verify the identity of a user and then allows the user to access some pre-defined resources, such as reading a file or executing an application. Usually an individual can be authenticated by his/her knowledge of a system or his/her physical characteristics. An assigned password is a traditional way for an individual to be authenticated by showing his/her knowledge of the system. Alternatively, keystroke biometrics is another way to perform authentication by human physical characteristics in terms of individual typing patterns. In this work, ‘individual typing patterns’ means inter-keystroke times are used as the authentication mechanism.

Authorizing a user to utilize certain resources is one of the main issues in secure distributed information systems. In this work, the distributed trust mechanism is introduced. Distributed trust means that a multi-lateral trust should be established among domains that enables users of one domain to access resources of other domains under a pre-defined mutual agreement. This agreement is referred to as *Foreign Policy* in each domain, which indicates the role-based access control information for foreign domain users. A role is assigned to a foreign user in his/her certificate issued by his/her host domain. The service domain will check its foreign policy to determine if the request is legal or not based on his/her role. A novel feature of authorization is its ability to balance the service quality for foreign users according to the current system workload. The system and the user may engage in negotiation in order to reach an agreement for a balanced point between the user’s request and the system resource expenditure.

In a distributed system, in order to keep message confidentiality and integrity, users are provided with different security measures such as encryption, decryption, digital signature and verification (Jonathan, 1998; Scott, 2001). It is desirable that user’s messages are protected from being viewed by unauthorized people in transit. To achieve this goal, symmetric and/or asymmetric cipher is used to encrypt the message at the sending end and decrypt it at the receiving end. Digital signature and verification provide users with assurance that a message has not been tampered and came from a specific person. These security services are time-consuming and need massive computation. To solve this