IGI PUBLISHING ITJ4170

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, **International Journal of Information Security and Privacy**, Volume 2, Issue 1
edited by **Hamid R. Nemati © 2008, IGI Global**

VIPSEC:
Virtualized and Pluggable Security Services Architecture for Grids[1]

Syed Naqvi, Centre of Excellence in Information and Communication Technologies, Belgium

ABSTRACT

Security of today's large scale, open, distributed heterogeneous systems (such as computational grids, peer-to-peer systems, pervasive/ubiquitous computing, etc.) has become a mainstream operational concern. Establishment of in-depth security services and trust relationships are the most desirable features for such systems. I have proposed a security architecture to address the comprehensive security needs of these systems (Naqvi & Riguidel, 2004a). Extensive groundwork was carried out to determine the limitations and shortcomings of the existing security solutions for these systems and to establish the real needs of the security architecture in order to reduce performance overheads and to provide robust security (Naqvi & Riguidel, 2004b). These include requirements analysis (Naqvi & Riguidel, 2005a), risk analysis (Naqvi & Riguidel, 2003), threat modeling (Naqvi & Riguidel, 2005b), and implementation feasibility (Naqvi, Riguidel, & Demeure, 2005).

Keywords: *distributed information systems; security management; trust issues; virtual organizations*

INTRODUCTION

Businesses have cooperated via computer networks since the early 1980s. These forms of cooperation were very static and took place in the form of electronic data interchange (EDI) (Kreuwels, 1990). Since the opening of the Internet for commercial use, more dynamic forms of cooperation are facilitated. However, the security needs of Internet-based systems are very different from those of traditional networking. For example, the Internet offers no centralized infrastructure to provide responsibility for network security. The security needs are particularly acute when high speed Internets are used to combine widespread computational resources. The best example of such distributed collaborative environment is the computational grid (Foster, 1998). A survey report of Virginia Tech in the fall of 2002 states that more than half of the grid community members believe that existing grid security solutions do not provide adequate services for collaborative grid communities. The reasons given ranged from the *lack of an underlying threat model* to the complexity and expense of inter-site trust relationships that are currently required (Lorch & Kafura, 2003). Sun Microsystems says adoption of global grids, where companies share hardware and software resources to accomplish a computational goal,

has been slowed because of security concerns and a lack of standards (Connor, 2002).

In the beginning of this century, various research funding agencies emphasized the need for a comprehensive research efforts of building scientific and technical excellences in security, dependability and resilience of systems, services and infrastructures, while meeting demands for privacy and trust (EU-IST; NSF). This research work is directly and indirectly supported by these research funding agencies.

PROPOSED ARCHITECTURE

Overview

In the large scale distributed systems, like computational Grid, the need for efficient and secure data transportation over potentially insecure channels creates new security and privacy issues, which are exacerbated by the heterogeneous nature of the collaborating resources. Traditional security approaches require adequate overhauling to address these paradigms. In this work, I propose a new two-pronged approach to address these security issues, VIPSEC (Virtualized and Pluggable Security Services Architecture). First, the virtualization of security services provides an abstraction layer on the top of the security infrastructure, which harmonizes the heterogeneity of underlying security mechanisms. Second, the configurable/pluggable nature of the various security services permits the users and resource providers to configure the security architecture according to their requirements and satisfaction level. This approach allows the security infrastructure to develop with minimal impact on the resource management functionalities.

Because security implementations are more and more numerous and complex, it has become almost impossible for an inexperienced user to understand their meaning and especially how they should be used. Additionally, the heterogeneity of networks does not simplify the understanding and definition of a security system. Therefore, it is currently impossible to establish a security policy for a communication by using the low level properties of the different networks that are being crossed. The classical solution to this problem consists in setting up a secured high-level ciphered tunnel from end to end. This is acceptable in some situations, but it may not satisfy future evolutions of networks. The goal of virtualization is to reinstate security principles (transparency, responsibility, traceability, etc.), security objectives (integrity, availability, confidentiality, etc.), security policies (protection, deterrence, vigilance, etc.) and security functions (identification, authentication, access control, management of secret elements, privacy, etc.) in their rightful place. Virtualization aims at describing a policy and at refining it. Actually, a unique security policy cannot be implemented on several heterogeneous networks, architectures or environments. The current complexity of networks comes from the fact that on the one hand each element defines its own security policy in accordance with the security domain to which it pertains (a priori…), and on the other hand each security domain has its own security policy. In the virtual paradigm, the policy of the element (wherever it may be) shall be merged with the policy of the domain to which it belongs. Then, this policy will be automatically implemented depending on the available security functions.

Virtualization

The concept of virtualization in information technology finds its roots in the very earliest software. The first programmable digital computers dealt in the world of 0s and 1s: Programs were 0s and 1s, output consists of 0s and 1s. As a result, programming was very difficult and programs were quite opaque. Then the compiler programs came into existence that let programmers work with English-like (high-level) languages like COBOL. The compiler took the COBOL code, crunched it, and spit out the 0s and 1s object code that the computers actually understood. The COBOL compiler, therefore, virtualized the object code.

As computers grew more powerful and complex, virtualization and encapsulation techniques continued to provide additional levels of abstraction. Timesharing mainframe computers