Chapter 11
Designing Efficient Security Services Infrastructure for Virtualization Oriented Architectures*

Syed Naqvi
Senior Member IEEE

ABSTRACT

Virtualization technologies are emerging as a promising solution for managing the rapidly growing complexities of modern distributed ICT infrastructures. However, a mainstream operational concern for these virtualization oriented architectures is to provide efficient security services. Establishment of in-depth security services and trust relationships are the most desirable features for the effective functioning of these systems. This chapter presents a security architecture to address the comprehensive security needs of today's virtualization oriented architectures. The concept of virtualization of security services is introduced so as to have absolute freedom to choose the underlying security mechanisms. This concept of virtualization of security services is realized through distributed virtual engines that enable unification of security service calls according to requirements and not according to the underlying technologies. A configurable mechanism for the invocation of security services is proposed to address the security needs of different kinds of users. This approach permits the evolution of efficient security infrastructure with minimal impact on the resource management functionalities. In this way, users and resource providers can configure the security services according to their requirements and satisfaction level. The resulting extensible set of security services include both core security services and contemporary security services required for the modern virtualization oriented infrastructures.

INTRODUCTION

The concept of virtualization in information technology dates back to the development of programming language compilers that were designed to virtualize the object code. Later virtualization emerged as cutting-edge technology not only for cost reduction of IT operations and support but also for ultimate simplicity, flexibility and agility of the underlying infrastructures. Server virtualization and consolidation are now regarded

DOI: 10.4018/978-1-61692-000-5.ch011

as top cost containment strategies by the majority of data center managers (Symantec, 2007). However, these emerging virtualization-oriented architectures give birth to several challenges for its deployment including a lot of uncertainty as to how and where to implement security (Adhikari, 2008). Although, initially security issues were not seen as bottleneck for the widespread adoption of virtualization-oriented architectures as overall security concerns are outweighed by the cost savings and operational benefits (Dignan, 2008). However, now it is expected that more attacks on the IT resources will take place with the increase in the number of virtualization-oriented architectures; and these architectures are going to face non-classical threats model that will require novel protection mechanisms for assuring the smooth running of their security operation procedures (Lewis, 2008).

In the recent years, 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, whilst meeting demands for privacy and trust (EU-IST; NSF). The work presented in this chapter has got direct and indirect support from these research funding agencies.

PROPOSED ARCHITECTURE

Overview

In the large scale distributed systems, such as computational Grids, Clouds, etc., 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. The two-pronged approach proposed in (Naqvi, 2004) to address these security issues is elaborated in this section. The proposed model is called VIPSEC: Virtualized and Pluggable Security Services Architecture. In this model, first, the virtualization of security services provides an abstraction layer on top of the security infrastructure that harmonizes the heterogeneity of underlying security mechanisms. Second, the configurable/pluggable nature of 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 be developed with minimal impact on the resource management functionalities.

Since 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.