Chapter VIII

Data and Application Security for Distributed Application Hosting Services

Ping Lin, Arizona State University, USA
K. Selçuk Candan, Arizona State University, USA

ABSTRACT

The cost of creating and maintaining software and hardware infrastructures for delivering web services led to a notable trend toward the use of application service providers (ASPs) and, more generally, distributed application hosting services (DAHSs). The emergence of enabling technologies, such as J2EE and .NET, has contributed to the acceleration of this trend. DAHSs rent out Internet presence, computation power, and data storage space to clients with infrastructural needs. Consequently, they are cheap and effective outsourcing solutions for achieving increased service availability and scalability in the face of surges in demand. However, ASPs and DAHSs operate within the complex, multi-tiered, and open Internet environment and, hence, they introduce many security challenges that have to be addressed effectively to convince customers that outsourcing their IT needs is a viable alternative to deploying complex infrastructures locally. In this chapter, we provide an overview of typical
security challenges faced by DAHSs, introduce dominant security mechanisms available at the different tiers in the information management hierarchy, and discuss open challenges.

INTRODUCTION

In an e-business setting, distributed computation with multiple parties’ participation is typical. Most business tasks, for example calculating the collective financial health of a group of independent companies, are inherently distributed (Franklin et al., 1992). Consequently, most businesses need an information technology (IT) infrastructure capable of providing such distributed services. For most businesses, investing in a local, privately owned infrastructure is not economically meaningful. For instance, an e-commerce company may find deploying an infrastructure that can handle peak demand volumes, while sitting idle most other times wasteful. Therefore, businesses are willing to pay premium prices for third-party solutions that can help them reduce their infrastructural needs while providing them appropriate quality of service guarantees. Consequently, application service providers (ASPs) and distributed application hosting services (DAHSs), which rent out storage, (Internet) presence, and computation power to clients with IT needs (but without appropriate infrastructures) are becoming popular. Especially with the emergence of enabling technologies, such as J2EE (J2EE, 2003) and .NET (.NET, 2003), there is currently a shift toward services hosted by third parties.

Most DAHSs typically deploy a large number of servers to host their customers’ business logic and data. They employ hardware- or software-based load balancing components to provide quality of service guarantees to customers. In addition, DAHSs can also place or replicate applications and data in servers closer to the end-users to eliminate network delays. Examples include Akamai and MirrorImage.

A typical application hosting infrastructure (Figure 1) consists of three major components: database management systems (DBMSs), which maintain business data, application servers (ASs), which encode business logic of the customers, and web servers (WSs), which provide the web interface between end-users and the business applications that are hosted by the DAHS. Although there are various modes of DAHS operation, a common way hosting services are used is as follows: (1) the customer (or application owner) with an application program publishes this application along with the relevant data onto the servers of the host. (2) Whenever they need, the customers (or its clients) access this application remotely by passing appropriate parameter variables to the host using the web interface. (3) User requests invoke appropriate program scripts in the
Related Content

Analysing Architecture and Transaction Model in Securing Mobile Commerce
[www.igi-global.com/chapter/analysing-architecture-and-transaction-model-in-securing-mobile-commerce/150076?camid=4v1a](www.igi-global.com/chapter/analysing-architecture-and-transaction-model-in-securing-mobile-commerce/150076?camid=4v1a)

A Survey of U.S. Laws for Health Information Security & Privacy
[www.igi-global.com/article/survey-laws-health-information-security/75321?camid=4v1a](www.igi-global.com/article/survey-laws-health-information-security/75321?camid=4v1a)

A Survey of Risk-Aware Business Process Modelling