Chapter XVIII

Aspect-Oriented Analysis of Security in Distributed Virtual Environment

Li Yang
University of Tennessee at Chattanooga, USA

Raimund K. Ege
Northern Illinois University, USA

Lin Luo
Florida International University, USA

ABSTRACT

This chapter describes our approach to handle security in a complex Distributed Virtual Environment (DVE). The modules of such an environment all need to be concerned about security. An object-oriented model of a DVE allows us to capture security in an aspect-oriented fashion as a crosscutting concern among the multiple modules. As DVEs become more complex in content, distribution, and capabilities, the security requirement emerges as a key issue in their design and implementation. In order to control the software complexity, our strategy is to model and analyze the impact of security concerns on the functional model of DVEs via an aspect-oriented technique. This approach is appropriate to be applied at both the system design and modeling stages and provides guidance during the implementation stage. This chapter illustrates an aspect-oriented approach to the impact analysis of security concerns upon the functionalities of DVEs. A design-level security model for DVEs is provided to show how to weave security concerns into the models of DVE designs seamlessly.

ASPECT-ORIENTED ANALYSIS OF SECURITY IN DISTRIBUTED VIRTUAL ENVIRONMENT

Distributed virtual environments (DVEs) are software systems that connect geographically dispersed users into a shared virtual space and support the interaction between the users and the shared world. DVEs have many applications in medicine, robotics, interactive distance learning and online communities. A DVE must satisfy a plethora of requirements so as to maintain realism of the virtual systems for all the users that are presently exploring this cyber environment.
More concisely, the environments should provide a sense of copresence to all participants, offer means for participants to communicate with each other or the world, respond to users' interactions, and support event handling.

As computing power and network bandwidth increase security, issues in DVEs become more critical and draw more attention. More and more DVEs involve sensitive areas (i.e., handle and produce proprietary or classified information, objects, and processes) security becomes a necessity. Given the richness and complexity of DVEs, there are a multitude of security issues requiring consideration during the development process. First of all, tens or hundreds of users may participate in a DVE simultaneously: all of them should be legitimate users as they access the virtual world. Second, a DVE often encompasses numerous multimodal data from multiple resources to provide a comprehensive and convincing 3D virtual space. Such data will contain rich multiple media like 3D graphics, text and streamed audio/video, and so on. Access to the media data may require different levels of confidentiality. Moreover, since participants interact with the system or other participants via advanced multimedia devices checking and enforcing of access privileges poses significant challenges. Any moment during their exploration of the cyberspace, they actively contribute shared information; this directly results in abundant yet frequently-updated data contributed and shared over the network. Such shared data may be a mixture of administrative flow, entity-data update, and streaming video/audio. Both the interaction and the information produced may be sensitive to some degree. In addition, since individual participants join and leave the shared space at will, changes of group membership happen frequently and further aggravate the management of security concerns. Finally, the transmission of the entire data stream, sensitive or not, may take place over untrusted networks where it is exposed to malicious attacks. In summary, adequate security handling is of increasing importance to allow DVE applications to flourish.

However, there is a lack of both analysis methodologies and techniques for DVE security due to the common preference to relax security in favor of performance. Since DVE applications normally entail frequent interaction, rich multimedia content and involve a great deal of distantly separated users, adequate handling of security significantly adds to latency and degrades the overall performance. This strategy was practical and efficient as most of the pioneering and experimental distributed virtual environments were built upon local or private network setting and the chance of a security breach was quite slight. But as distributed virtual systems widely spread from dedicated networking links to unsecured public networks, a higher need for security concern in the design and implementation of DVEs is inescapable.

This chapter provides an approach to analyze the impact of security concerns in DVEs and to weave the requirements into the environments using an aspect-oriented technique. We elucidate how to model design-level security concerns and how to encapsulate them into DVE design models.

The rest of the chapter is organized as follows. First, we outline related efforts regarding security in DVEs. Then we present an object-oriented view of the distributed virtual content and our evolution of a role-based access control security model. The aspect-oriented analysis of the security capability within DVEs is described in the next section, along with the overall woven results. Finally, we summarize and conclude with perspectives for further work.

**RELATED WORK**

Much research has been conducted on the subject of security and has resulted in copious techniques and approaches to address the issue from different views and to different levels. The key to the development and integration of a secure infrastructure is information assurance (IA), which has five focal pillars: availability, integrity, authentication, confidentiality, and non-repudiation. As a challenging, complicated and sensitive application, a DVE is influenced by all five subjects of IA at varying levels throughout its life cycle.

Despite its importance, security research specific to DVEs has been somewhat limited compared with the fairly well-researched general security of computer systems and networks. In the 30-year evolving history of DVEs, security was usually treated as of lower priority in contrast to performance and reliability issues. In most of the notable early DVE efforts, the security issues rested primarily with dedicated networks with fully trusted users. A good example is SIMNET (Miller & Thorpe, 1995) sponsored by the U.S. Department of Defense. As the first successful implementation of a large-scale real-time DVE, SIMNET utilized dedicated, high-speed networking links to interconnect its participating nodes. As DVEs evolved progressively,
Related Content

Blind Image Source Device Identification: Practicality and Challenges
[www.igi-global.com/article/blind-image-source-device-identification/208127?camid=4v1a](www.igi-global.com/article/blind-image-source-device-identification/208127?camid=4v1a)

Information Security Management
[www.igi-global.com/chapter/information-security-management/23098?camid=4v1a](www.igi-global.com/chapter/information-security-management/23098?camid=4v1a)

Libraries to the Rescue
[www.igi-global.com/article/libraries-to-the-rescue/148214?camid=4v1a](www.igi-global.com/article/libraries-to-the-rescue/148214?camid=4v1a)

A Flexible Authorization Framework
[www.igi-global.com/chapter/flexible-authorization-framework/23156?camid=4v1a](www.igi-global.com/chapter/flexible-authorization-framework/23156?camid=4v1a)