XMSF Security: XML and DRM Issues

Chenghui Luo, Ph.D.
Fraunhofer CRCG, Inc.
321 South Main St.
Providence, RI 02903
cluo@crcg.edu

1. XMSF: An Introduction

E**X**tensible **M**odeling and **S**imulation **F**ramework (**XMSF**) is a web-based modeling and simulation framework that is designed to support development, analysis and training of operational tactical systems as well as commercial applications. In a military scenario, XMSF will enable better simulation and coordination of all operational tactical resources and in a business environment, XMSF will support better collaboration in the product design and development process that is essentially distributed with the globalization of modern economy. XMSF will also support the interoperability in a large network of legacy modeling and simulation systems.

XMSF is currently proposed and to be developed by a consortium of academic, industrial and governmental researchers and developers. To succeed in this effort, two important technical issues, i.e., interoperability and security must be solved. In this note, we discuss the security issue of XMSF.

2. XMSF Security: XML Issues

Typically, an XMSF application is distributed on a network of computers and the first security requirement is secure transmission and proper access of data. Thanks to modern cryptography, symmetric and public key cryptographic systems have been developed, authentication and digital signature schemes have been established, network security technologies such as firewalls are now running on various kinds of systems. All of these provide a good foundation for robust XMSF security.

At an application level, however, on top of these security technologies, access control techniques such as authentication and authorization must be well designed and integrated to support secure interoperability in the web-based XMSF framework. Web services are the programmatic interfaces for the applications on the web and it holds the promise to support better interoperability. XML (eXtensible Markup Language), an important component of web services, presents a standard way to exchange structured and formatted information in environments that do not share common platforms in a distributed application. In this web services and XML scenario, XMSF data and services can be represented using XML-based web services technologies, and the XMSF security problem can be partially solved by XML security technologies. Currently, there are a few XML-related security technologies such as XML encryption, XML signature, eXtensible Access Control Language (XACL), Security Assertion Markup Language (SAML) and XML Key Management Specification (XKMS). These efforts are good starts for XML-based XMSF security.

But up to now, there is no XML-based markup language specifically designed for the modeling and simulation purpose. Web 3D (VRML) and its new iteration X3D are not based on XML at all, and there is no application level security mechanism defined in either Web 3D or X3D. For the success of XMSF, a special purpose XML-based modeling and simulation markup language must be created, and an application level security mechanism must be designed and developed afterwards. From this point of view, there is a long way to go for XMSF security.

3. XMSF Security: DRM Issues

Although proper XMSF security can de developed based on XML-based access control techniques, there is another side of the XMSF security issue: intellectual property rights (IPR) such as trade secrets and copyrights. The IPR issue of XMSF is different from the transmission and access control aspect of security in that in a military or business application, the original sender (owner) of the secret or sensitive data may still want to maintain some control of the data even after it's securely transported and decrypted. In a typical distributed application including XMSF, this aspect of security is out of the original owner's control after a secure transmission, because that information is now accessible to and totally within the discretion of the recipient, or any illegal access to the recipient.

One approach to this IPR issue is called digital watermark, which is to embed a secure invisible label in a digital content. However this is basically not a proactive approach because it generally can only provide evidence of misuse after the misuse happens. A broader approach falls in a category called Digital Rights Management (DRM). A DRM system may actively control the proper use of information such as what, where and how long to use. In a DRM approach, typically a wrapper will be developed and applied to the information, and the protection mechanism is enforced by a component installed and running on a client end. This way, the original owner can maintain its control of the information even after a transmission.

The DRM approach may present some inconvenience or interoperability drawback to the XMSF framework, but as long as the information is not absolutely open to the whole world, there must be some trade-off between security and convenience. Beyond that, the DRM approach supports a broader scope of fine-grained security features, which is good for many commercial and military applications. For example, we can develop a multi-resolution, multilevel system to control the access rights to a secret model or information; or we can deliver only a few 2D projections so that it's almost impossible to reconstruct the original 3D model based on the few 2D projections. All of this extensible, customizable functionality can be well integrated in the wrapper of a DRM system. In XMSF, this wrapper can be integrated with a viewer, which is typically required in modeling and simulation applications.

DRM is an active research and development area, its requirements for the modeling and simulation scenario must be clearly understood, and a DRM-based security enforcement system is still to be developed.

4. Conclusion

XMSF is a web-based modeling and simulation framework that is designed to support interoperable development, analysis and training of large distributed applications. Current cryptographic technologies have provided solid foundations for XMSF security such as XML-based encryption, authentication and digital signature, but an XML-based modeling and simulation language is still to be designed and major research and development on digital rights management for the modeling and simulation scenario is still needed to make it a secure framework for military and business environments. Government funding to this framework will make XMSF securer and a success.