Chapter 10

X3D: A Secure ISO Standard for Virtual Worlds

Joerg H. Kloss
X3D Consultant and Expert, Germany

Peter Schickel
Bitmanagement Software GmbH, Germany & Web3D Consortium, Germany

ABSTRACT

This chapter discusses the topic security in standard based virtual worlds with emphasis on X3D as the international ISO/IEC standard for Virtual Worlds. The general security challenges in persistent and economic virtual environments are addressed as well as the importance of standardization and security as the two key success factors for reliable, cost-effective and long-term attractive Virtual World (VW) platforms. Different actual standardization approaches are compared to the established X3D format that follows a clear security standardization path. Based on the Internet standard XML the specific advantages of X3D are emphasized, such as seamless integration into Web applications and deployment of generic XML tools. The generation of encrypted and signed X3D binary files is demonstrated according to the XML Security Recommendation of the W3C consortium. In a practical session the appliance of security approaches to concrete X3D implementation projects is described from the perspective of Bitmanagement, a market leader for interactive Web3D graphics software.

INTRODUCTION

X3D is a powerful description language and open data format for high-end real-time 3D graphics, animation and interaction dedicated to Web-based and other professional 3D applications. It is an international ISO/IEC standard, designed and maintained by the Web3D consortium, with origins in the VRML standard, and widely-used within different scopes, like e.g. scientific visualization, virtual and augmented reality, geographical information systems and Virtual Worlds. Due to its specific characteristics as a human readable web description language like XHTML, the Web standard X3D offers similar advantages, but is confronted with challenges like security. In consequence the current specification for HTML 5 states that embedding 3D imagery into XHTML...
documents is the domain of X3D, or technologies based on X3D that are namespace-aware (W3C, 2009).

If it comes to the question of security in X3D-based Web applications and VW’s there are many issues similar to those with other VW technologies and approaches, some that are related to the general discussion of the World Wide Web Consortium (W3C) standards, and some others that are quite specific to X3D itself. Further on there are individual security solutions developed by companies working with X3D day-to-day. This chapter will shortly address some of these different aspects, but will focus on the X3D specific approaches and will present a concrete example of the security solution applied by the 3D viewing technology company Bitmanagement. The reader gets an approximate overview about security aspects in VW’s, becomes acquainted to the specific approaches in X3D, and finally learns how security is applied to real-world X3D applications today.

BACKGROUND

The question of security in VW’s is manifold. This is even more comprehensive when it comes to persistent VW’s that include economic systems with virtual currencies, which are connected to real-world markets and money. And it applies likewise to massively multiplayer online games (MMOGs), social as well as corporate worlds. With the rise in success, members, virtual goods and economical power of a VW, also the potential for misuse and attacks increases. The list of possible risks is long and in no case complete: avatar identity fraud, theft of virtual and intellectual properties, disclosure of private data, cheating in trading and by illegal object duplication, harassments and threats to minors, vulnerabilities to platforms by spam and denial of service (DoS) attacks and so on.

Most of these challenges are not even fully captured yet, and cannot be solved just technically. Furthermore, many VW’s are based on closed systems with individual architectures as well as proprietary data formats, which makes it even harder to define, apply, and establish a general security approach of trust.

INDUSTRY STANDARDS AND PROPRIETARY TECHNOLOGY

However, with a reliable, independent, and transparent standard, investments into VW’s could become more ‘secure’ also from an economical point of view. To overcome the prevailing multitude of proprietary technologies and privately held platforms, different standardization approaches are currently under development (Behr, 2009).

SUN Darkstar

A popular virtual worlds server is provided by the Darkstar project from SUN (SUN, 2009). In a strategic whitepaper SUN confirms that due to major technical differences of virtual worlds platforms open standards are needed in this domain and states that X3D is one possible solution here (SUN, 2008).

Google O3D

With a focus on 3D Web graphics Google released their proprietary browser plug-in “O3D” (Google, 2009b). Their target audience are JavaScript programmers who need the flexibility of a low level graphics API. However it does not provide a method to define the content in a declarative way. Application developers have to use JavaScript code to manipulate the behavior of their content, which is considered slow, because it needs to be interpreted at runtime. With regards to security there is no specific encryption path foreseen as all parts of the application logic and behavior have to be entirely programmed in JavaScript.