

# Technology **Today**

HIGHLIGHTING RAYTHEON'S TECHNOLOGY

2008 ISSUE 3

## **Raytheon's Net-Centric Communications**

Building a Foundation for Innovative Solutions



**Raytheon**

*Customer Success Is Our Mission*

# Information Assurance in a Virtual World



## Virtual World Technology: What Is It?

Virtual reality, or virtual world, technologies are not new. Many of us were first exposed to this domain through the book *The Metaphysics of Virtual Reality*, by Michael Heim. In this book, Heim identifies seven different concepts of virtual reality: simulation, interaction, artificiality, immersion, telepresence, full-body immersion and network communication. Hollywood first made this idea popular through Steven King's *The Lawnmower Man*. Other futuristic examples can be found in popular media such as *Star Trek* with its "holodeck" and *The Matrix*, where a "head-plug" was used to place individuals in a simulated reality<sup>1</sup>.

Virtual world technology and the capabilities it provides allow users (humans) to interact with a computer-simulated environment. The environment may be based on real-world scenarios, such as a corporation's human resources or training organizations, or imaginary, such as those typically found in action games. The quality of the virtual

reality experience is based on the sophistication of the software applications and the inherent computer and image processing power available. Additionally, in distributed environments, such as for telemedicine, the available communications bandwidth can play a dramatic role in the usability of the system. Initially, virtual reality-based systems were primarily visual in nature. However, recent advances enhance the experience through audio, touch and smell. Such feedback capabilities are critical to the experience, especially in medical and gaming applications.

Users interact with the virtual environment through input devices that now range from a keyboard and mouse to neural-based sensory devices that users wear and, through their thoughts, control their interactions with the virtual environment. Output devices include high-fidelity stereophonic headphones or loudspeaker systems that nearly make the listener believe they are actually there, to odor-delivery systems. Some of the

most interesting work in the area of simulating visual, audio, smell and touch is in the treatment of post-traumatic stress disorder in veterans. By exposing them to combat simulations, complete with smells, it is possible to provide treatments that address directly those feelings and fears that haunt these servicemen and women.<sup>2</sup>

The technologies that make virtual reality a usable and inherent part of society continue to move forward. However, it is unclear what the future holds. The most popular forum for virtual world capabilities today lies within a hosted environment called Second Life®. In a recent interview by Cisco Systems, Inc., CEO John Chambers appeared at a virtual press conference in Second Life and predicted that virtual world technologies will "explode" for business usage and make significant impacts in society. Google recently also unveiled its own virtual world, called Lively. Lively allows its members to create avatars, decorate their own virtual rooms, invite friends to their "rooms," and

do things that one would not normally do in the real world, such as fly to the moon.

### Virtual Worlds – Why Are They Important?

Virtual worlds and virtual reality technologies are growing in importance not because of their entertainment value, but because they are also becoming critical tools within the U.S. military and intelligence communities for training and other purposes.

The implication of this is twofold. First, should the U.S. military increase funding for furthering the use of virtual reality? The answer for this question has become obvious based upon recent investments by the U.S. Department of Defense (DoD). The DoD is reportedly planning to build a virtual world called “Sentient Worldwide Simulation.” The objective of this system is to mirror the real world and automatically follow world events in real time. In addition, both JFCOM (Joint Forces Command) and TRADOC (Training & Doctrine Command) are using virtual world technologies to provide training environments targeted at developing skills in urban warfighting operations.

Second, recently released intelligence data indicates that our adversaries are also using virtual worlds to provide terrorist organizations with more realistic training environments. This finding possibly allows U.S. intelligence organizations to gain valuable insight into the behavioral aspects of our adversaries.

As the use of virtual world technology spreads through the military and intelligence services, the concern over the threats and risks that this new technology presents become paramount in terms of the entire enterprise. Virtual reality is based primarily on Web content capable of supporting three-dimensional views. This is made possible through the use of Web 2.0. Web 2.0 is a second-generation language used to create communities, or social networks, where content is not just viewed, but where a user can dynamically create, modify and share Web content. Web 2.0 and virtual reality technology presents numerous challenges to maintaining a secure infrastructure.

### Virtual Worlds – What Are the Risks?

Risks lie primarily in two areas. The first centers on the use of Web 2.0 for interactive Web content. The second lies with the underlying technologies used for authentication, confidentiality and integrity services. Web 2.0 applications can be divided into three categories: rich interface applications, syndication, and user participation. Each of these introduces its own set of vulnerabilities and risks. Protecting against session and cookie tampering, SQL injection, directory traversal, and cross-site scripting-attacks becomes significantly harder to prevent. The result is a much broader attack space as the security processing moves from the Web server to the client.

Providing authentication, confidentiality and integrity take on a new level of complexity with virtual reality. Techniques normally used in standard information-management environments do not provide the necessary dynamics to deal with authentication of users and their associated avatars, or providing confidentiality and integrity for virtual reality communities and their associated content.

When using virtual worlds in the military and intelligence areas, capabilities such as data encryption, biometrics, malware detection, digital signatures, identity rights management, etc., must be used to validate user activities in the virtual world. Auditing all ongoing transactions becomes infinitely more complex as the collected log files must be aggregated, correlated and validated against potentially millions of virtual reality objects.

### Why Is Raytheon Investing in Virtual Reality?

As part of Raytheon’s overall research and development investment strategy, virtual reality and virtual worlds have surfaced as prime candidates for investment, because of their direct applicability to many of the training and weapon systems Raytheon delivers. Additionally, virtual reality is viewed by many as a technology that is still in its infancy, and thus it represents a new domain where Raytheon can add value

by applying new capabilities it is developing in information operations and information assurance.

Through virtual reality, Raytheon believes it is able to make significant strides in the methods by which its customers can be trained on the various complex mission systems it delivers. As a premier Mission Systems Integrator, Raytheon continuously strives to enhance its solutions through the introduction of innovative technologies and methods. Through virtual reality, Raytheon believes it can significantly reduce the cost of system development and user training, and dramatically improve a user’s proficiency in a shorter time period.

Before this is possible, however, new advancements must be made in the security features of virtual reality environments. Raytheon’s initial investments in virtual reality are targeting those challenges with pervasive identity rights management within a virtual world. Ensuring that users’ identities are not stolen, cloned or otherwise impersonated are critical to ensuring the confidentiality and integrity of the services provided through a virtual reality environment. Raytheon is leveraging previous research in its Compartmented High Assurance Information Networking architecture to develop new access-control and identity-rights methods that can be applied at the avatar level.

Raytheon’s objective is to develop of suite of solutions that can be applied to virtual reality through internal research and development and by collaborating with academia to advance the methods used today. ●

Dan Tejjido  
dant@raytheon.com

<sup>1</sup> Wikipedia, The Free Encyclopedia. “Virtual Reality.” July 22, 2004, 10:55 UTC. Wikimedia Foundation, Inc. <[http://en.wikipedia.org/wiki/Virtual\\_reality](http://en.wikipedia.org/wiki/Virtual_reality)>

<sup>2</sup> Wilson, Clay. Foreign Affairs, Defense, and Trade Division, Congressional Research Service. “Avatars, Virtual Reality Technology, and the U.S. Military: Emerging Policy Issues,” April 9, 2008.

Second life is a registered trademark of Linden Lab.

Copyright © 2008 Raytheon Company. All rights reserved.

Approved for public release. Printed in the USA.

*Customer Success Is Our Mission* is a registered trademark of Raytheon Company.

Raytheon Six Sigma, MathMovesU and NoDoubt are trademarks of Raytheon Company.

MATHCOUNTS and Mathletes are registered trademarks of the MATHCOUNTS Foundation.  
Capability Maturity Model, CMM and CMMI are registered in the U.S. Patent and Trademark  
Office by Carnegie Mellon University.

**Raytheon**

*Customer Success Is Our Mission*