

The National Academies  
Workshop on  
***Usability, Security, Privacy of Computer Systems***

**Topical Issue:**  
**Security in Virtual Worlds**

Frank L. Greitzer, PhD  
Chief Scientist, Cognitive Informatics  
Pacific Northwest National Laboratory  
Richland, WA 99352  
[frank.greitzer@pnl.gov](mailto:frank.greitzer@pnl.gov)

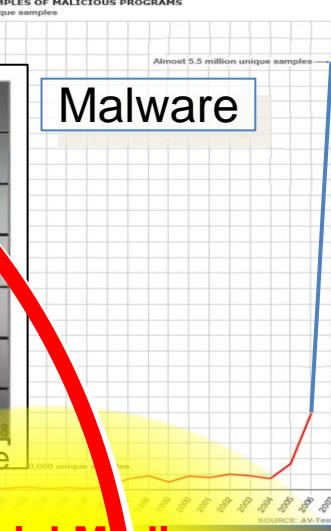
July 2009



*Proudly Operated by Battelle Since 1965*

# Security and Privacy in an Expanding Cyber World

**“Mouse click could plunge city into darkness, experts say.”**  
--CNN.com, Sept 27, 2007



Identity Theft:  
\$50B per year in U.S.

MMOGS



Insider attacks:

- 2<sup>nd</sup> greatest cybersecurity threat (E-Crime Watch (2004))
- 5<sup>th</sup> most serious security menace (Sans Institute, 2008)

Social Media:  
Blogs, Microblogs  
(e.g., Twitter),  
Social Networking  
sites  
(e.g., Facebook).



Pacific Northwest  
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

# Security and Privacy in an Expanding Cyber World

## Virtual Worlds

*What are security issues in virtual worlds that threaten privacy and trust in these environments?*

# Security and Privacy in Virtual Worlds

*What happens when forces for  
“digital trust” collide with interests  
in safeguarding the security of  
information systems?*

# Security and Privacy in Virtual Worlds

*Usability and Security:  
Fundamental “system induced  
user errors” point to system  
design deficiencies.*

# Virtual Worlds: Nature of the Threat

- ▶ Virtual Worlds transforming business practice
  - Businesses require confidentiality (Second Life is open, not private): IBM's **Metaverse** is an internal virtual world for corporate meetings and collaboration)
- ▶ What are similarities and differences between needs and challenges associated with security in virtual worlds versus grid or cloud computing?
- ▶ Challenges
  - Lack of sophisticated security models
  - Encryption and authentication
  - Social engineering
  - Psychological engineering

# Virtual Worlds Security Fears

## ► **Identity and access management**

It's difficult -- if not impossible -- to ensure that any avatar is the real-life person it claims to be. This has a significant impact on the potential use of virtual worlds for collaboration purposes

## ► **Confidentiality**

Open, Internet supported social-networking sites do not provide adequate security/privacy. Discussions involving confidential and commercially sensitive information should be moved to a private virtual world where the issues of privacy, confidentiality and identity can be controlled.

## ► **Brand and reputation**

Uncontrolled virtual worlds represent an environment "fraught with danger" for enterprises that are sensitive to brand and reputation issues.

## ► **Productivity**

Many senior executives view virtual worlds as a waste of time and bandwidth resources—is this generally true except for gaming? When does it enhance productivity? What are tradeoffs between their use and associated security risks?



**Pacific Northwest**  
NATIONAL LABORATORY

# R&D Challenges: Conventional Cybersecurity

## Encryption and authentication

- ▶ What sort of authentication/credentials might be the most appropriate in virtual worlds?
  - Certification/private key
  - “Virtual Biometrics?”
- ▶ Who should be responsible for managing credentials and verification?
  - Individuals responsible—carry a credential wallet with certifications and keep a private key with them?
  - Centralized approach would require that the credential wallet contain redirections to a trusted entity (e.g., university, hospital) – this removes responsibility of control from user
  - Hybrid approach could combine attributes of individual and centralized approaches.



# R&D Challenges: Human Factors

- ▶ Find potential solutions that promote security, preserve privacy, and raise trust
  - How to manifest authentication/certification in virtual worlds that will be effective and successful from a human factors perspective? [reliability/ensure privacy/confidentiality]
  - Engineering issues must be addressed in psychologically acceptable ways.

*How can we make a solution **USABLE** and **TRUSTWORTHY** for individuals who participate in virtual worlds?*

# R&D Challenges: Validation

How can we evaluate the effectiveness of proposed solutions?