Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2007

Security Issues within Virtual Worlds such as Second Life

Chia Yao Lee
Deakin University

Matthew Warren
Deakin University

Originally published in the Proceedings of 5th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, December 4th 2007
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/44

Security Issues within Virtual Worlds such as Second Life

Chia Yao Lee and Matthew Warren
School of Information Systems,
Deakin University,
Victoria 3125, Australia
chia.lee@deakin.edu.au
matthew.warren@deakin.edu.au

Abstract

The advancement in Internet and bandwidth has resulted in a number of new applications to be developed. An area of advancement has been in the development of virtual worlds, where people can interact together via virtual characters. Virtual World systems have been so complex that virtual lives can be lived, including all aspect of life such as education, commerce, social activities etc. Not surprisingly, the problems that exist in the real world such as theft, fraud, vandalism and terrorism, also exist in the virtual worlds. The more developed these virtual worlds become the greater the breaches of security will be in the virtual as well as the real world.This paper explores and categorises several security issues within the Virtual World of Second Life. It contributes to practice and research by emphasising the importance of security awareness for businesses and the general public in Virtual Worlds.

Keywords

Virtual World and Security Issues.

INTRODUCTION

Information access any time, any where, any place. While Electronic Business (e-business) provides access to business and commerce to anyone at anytime from a networked desktop computer, and Mobile Commerce provides the next dimension, with access to anyone from any where – not just the fixed desktop, but also from the highway, the restaurant and the beach through wireless networks. The emergence of Virtual Worlds as a platform for business and commerce extends e-business to the domain of 3D virtual reality (Bray and Konsynski 2007; Hemp 2006). Many have claimed that business in Virtual Worlds may supplement, complement and even extend existing e-business and m-commerce activities (Hof 2006). Virtual Worlds are self contained 3D graphical worlds on the Internet. Examples of Virtual Worlds include Active Worlds, Entropia Universe, There, Home, Second Life, World of Warcraft etc. Within these self contained computer based worlds, users can use avatars to interact with other users, as well as with various elements of virtual environment. An avatar is a virtual representation of the user through which an interaction with the virtual world system is made (Barbagli et al, 2004).

In many ways Virtual Worlds such as Second Life are a representation of the modern society. In terms of housing and real estate, education and training, media and entertainment etc, almost all aspects of the economy and society have been mimicked and replicated in Virtual Worlds. Shopping (Salomon 2007), socialising, attending university, celebrating virtual weddings and volunteering for charity causes are some of the popular activities in Virtual Worlds.

In terms of this paper, the research team has focussed upon considering the security issues within the Virtual World of Second Life. The reason for this is the rise in popularity of this particular virtual world and the increasing number of security issues which have arisen in recent months. The study also seeks to better understand security issues that may cause serious disruption to e-business and other key activities in Virtual Worlds.

SECOND LIFE

Second Life is a 3D virtual world developed by Linden Research Inc., commonly referred to as Linden Lab, but many elements within the Second Life environment, the Second Life Grid, are developed and owned by Second Life residents. Since opening to the public in 2003, Second Life has grown and today has close to 10 million

residents from around the globe (Second Life, 2007a) although not all of the 10 million residents participate actively. To become a Second Life resident, a user may opt for a premium account that incurs an ongoing subscription fee or sign up for a basic account that is free of charge but comes with limited features and capabilities. To access the Second Life Grid, residents will need to run the Second Life Viewer, a client application that operates much like a 3D Internet browser.

Unlike other Virtual Worlds such as the World of Warcraft, Second Life has attracted the attention of major multinational companies, government agencies, practitioners and researchers due to the existence of its active virtual currency and economy (Bray and Konsynski 2007). On average, Second Life records US$1 million in business transactions each day. Linden Dollars is the official currency in Second Life. Several online resources allow residents to convert Linden Dollars into US Dollars and vice-versa. The currency conversion rates fluctuate based on supply and demand of the virtual world currency, but over the last few years they have remained fairly stable at approximately 250 Linden Dollars (L$) to the US Dollar (Second Life, 2007b).

A snapshot of the Second Life economy in August – September 2007 is shown in Figure 1 (Second Life, 2007c).

Month	Total Square Meters Sold by Residents	Average L& Paid Per Square Meter
August 2007	74,491,264	7.0839
September 2007 MTD	3,277,808	6.9419

Figure 1: Land Sales by Residents in August/September 2007

The total supply of Linden Dollars (L$) within the Second Life Economy is L$3,311,370,557 (Second Life, 2007c) in 2007. Second Life has gradually developed into a relatively mature 3D virtual reality environment.

The following aspects of the modern society have taken place in Second Life:

- **Entertainment and Arts** – Virtual entertainment events have been staged in Second Life. These events are commonly sponsored by Second Life businesses. Residents may need to pay a fee to access some of these events. Such entertainment events take the form of musical rock concerts, such as an avatar based version of U2 (www.u2insl.com), or participation in role-playing games. Machinima, a genre of cinematographic film produced within Virtual Worlds, represents another aspect of entertainment and arts which has attracted substantial interest among real world companies. In September 2007 HBO has purchased the rights to a film produced within Second Life. The machinima is expected to be released in 2008 (Reuters 2007).

- **Commerce** – Many real life multinational companies have extended their business services to existing customers who are also Second Life residents (Salomon 2007). Companies such as IBM and Cisco have established a Second Life customer service centre. These virtual world contact touchpoints are intended to be a virtual place where clients, potential clients and partners can browse products and offerings, seek technical guidance or interact with company representatives (Hutcheon, 2007a).

- **Education** – Dozens of universities and higher education institutions are opening campuses in Second Life as a way of delivering their educational programs to the community. A number of universities around the world have established virtual campuses in Second Life to enable students to work collaboratively, e.g. Ohio State University (Ohio State University, 2007), while others have gone to the extent of conducting programs within Second Life, e.g. Harvard University's CyberOne: Law in the Court of Public Opinion course (Harvard Law School 2006).

- **Government and Politics** – Real world government agencies have used Second Life as a channel for communicating with the public. The Swedish government has established a virtual embassy in Second Life to promote tourism and cultural exchange (Courier Mail, 2007). There exists a virtual U.S. Capitol in Second Life (Reuters 2007b) which was used to video-stream the opening of the 110th Congress (Reuters 2007c). Several American presidential candidates like Barack Obama and Hillary Clinton have virtual campaign offices within Second Life. The First National political party in France brought its election campaign into Second Life in early 2007(Guardian 2007). Avatars supporting and opposing the First National party have launched vicious griefing attacks on one other in the Virtual World.

LIMITATIONS OF SECOND LIFE

As promising as the Second Life platform may be, it contains several limitations which have been cited as the major stumbling blocks that are preventing it from gaining greater acceptance among businesses and the general public (Salomon 2007). The following details some of the major limitations of Second Life.

1. The Internet bandwidth and hardware requirements for accessing Second Life are high. A cable or DSL Internet connection is the minimum requirement for accessing the Second Life grid. The graphic-intensive nature of the Second Life Viewer application also limits access to users who are equipped with the latest computing hardware. As such not every Internet user will have an equal access to Second Life.

2. Reliability and stability of the Second Life Grid. The Second Life Grid is taken offline for maintenance and upgrades regularly. The Grid has a service performance with just above 90% service availability (Reuters 2007c). As Linden Lab's CEO Philip Rosedale has admitted, there is still much room for improvement (Reuters 2007c). Unscheduled downtime for fixing bugs and errors may frustrate even the most patient individual users, if not create serious repercussions for businesses within the virtual world. The Second Life Grid may also suffer performance problems such as laggy responses if there is an overcrowding of an island or region.

3. The complexity of the Second Life Viewer application. Many new Second Life residents will need to spend a few hours to familiarise themselves with the application. The application is not as simple or intuitive as the more widespread web browsers and email clients that Internet users are already familiar with. The issue has been addressed partially by the recent launch of OnRez (www.onrez.com), an alternative Second Life viewer developed by the Electric Sheep Company.

4. Lack of corporate governance in Second Life. The recent collapse of a pre-eminent bank in Second Life has impacted thousands of residents who have deposited funds in the bank (Hutcheon, 2007b). The lack of corporate governance and business regulation within Second Life may leave consumers and businesses with little protection against fraudulent business and greatly reduce the level of confidence and trust in Second Life businesses.

5. The emptiness and loneliness of the Second Life Grid. Many Second Life critics have argued that the Second Life Grid is empty and marketers are not getting good returns for their investment if their virtual world creations are not visited (Rose 2007). Marketers are learning now that it is not a simple case of "Build it and they will come". A a more important issue lies in aligning the objectives of Second Life business operations with a company's core processes and objectives.

6. Open sourcing of Second Life. At the moment, the Second Life Grid is operated and controlled wholly by Linden Lab. Businesses in Second Life are not able to host their Second Life islands (and thus their operations) on their own computer servers. On the 2D Internet businesses could own and operate their own web servers, email servers and security firewalls. Since Second Life Grid is operated much like a proprietary network, businesses operating in Second Life have little control over the access and availability of the grid. The recent open sourcing of Second Life viewer, and the hosting of alternative grids by 3rd parties may overcome several limitations detailed above.

7. Lack of integration with other Internet applications and other Information Systems. At present, the Second Life Grid is not integrated with other online applications residing on the traditional 2D Internet. Whilst it is possible to stream videos or RSS feeds into Second Life, businesses are unable to integrate their Second Life applications with their internal information systems, e.g. Enterprise Resource Planning systems.

The research team believes that while several of the above limitations may be addressed by Second Life developer Linden Lab and Second Life residents in due course, a greater concern remains in the area of security in Second Life. Recent incidents whereby Second Life events were disrupted, avatars were attacked, and virtual properties were misused or damaged, suggest that security in Second Life is an issue that residents and businesses will need to pay attention to.

SECOND LIFE SECURITY ISSUES

The Virtual World Security Threat Matrix

Based on an analysis of security incidents reported in the business and academic press, the research team proposes a modified version of the Virtual World Security Threat Matrix (Lee 2007), as illustrated in Figure 2 below, to better understand and analyse security issues that exist in the virtual world of Second Life. The research team proposes to modify the framework by adding two additional security dimensions - (i) Payment and Transactional Integrity, and (ii) Malwares and Computer Virus, to the existing list of six. Another modification involves the inclusion of a column to detail a real world analogy. The research team acknowledges that the modified framework may not be exhaustive in identifying all the different security dimensions but at the very least it provides a broad overview of security issues that affect Second Life residents, organisations, and community. It is important to note also that the security dimensions are not listed according to any order of importance.

Security Threat Dimension	***Nature of issue***	***Description/Real World Analogy***	***Implication***
I. Privacy & Confidentiality	▪ Information exchanged and transmitted between avatars may not be private. Text chat, voice chat and private instant message between avatars are not encrypted. ▪ Automated and manual applications may be used to record and listen in to conversation between avatars without the expressed consent of avatars. ▪ Avatar activities, virtual environment and virtual objects (e.g. the trail of an avatar, the appearance of a 3D design) may be monitored and video-recorded without expressed consent of the owner/avatar.	▪ Snooping and sniffing to capture information (electronic or otherwise) transmitted at the workplace and home ▪ The behaviour and trail of shoppers may be monitored and analysed by a merchant either through in-store video cameras, or through customer loyalty programs. ▪ Commercial-in-confidence materials are commonly discussed in secure premises, or via secure channels, to avoid eavesdropping.	▪ Organisations (and possibly government agencies) will need to develop guidelines and policies to determine what information may/may not be discussed in Virtual Worlds, and how stakeholders will be notified if they are being monitored. ▪ Avatars need to be educated on the ethics of communication in Virtual Worlds, and on how to avoid snooping applications, how to sweep a virtual environment to look out for hidden monitoring devices. ▪ Companies such as IBM have established guidelines that restrict employees from discussing commercial-in-confidence information within Second Life.
II. Authentication & Identity Theft	▪ Verifying the identity of an avatar identity. Similar to social networking sites, identity theft may be possible if social engineering techniques are used to reconstruct the profile of an avatar, leading to identity theft. ▪ Verifying the identity of owners/creators of virtual objects –	▪ Multi-modal authentication and verification methods are used for Internet banking. ▪ Passport details, physical addresses and phone numbers may be required for communicating with government agencies and conducting Internet e-Business, e.g. booking air travel.	▪ Some businesses in Second Life have organised for employees to use a similar avatar last name, e.g. all Cisco employees have "Cisco" as their avatar last name. ▪ Some businesses in Second Life have resorted to using non-Second Life applications for identity verification, e.g. paypal accounts. There have been cases where avatars falsely collect rent from customers, or purporting to be

	creator of a virtual product, landlord of a virtual location. Phishing in virtual worlds? ▪ Apart from credit card registration for identity verification (as supported by Linden Lab currently), other mechanisms are not available. ▪ Age-check mechanisms are needed to protect minors. Currently, minors can only access the Teen Grid, how to prevent adults from accessing the Teen Grid? How to prevent minors from accessing the main grid?	▪ Internet websites use certificates for authentication purposes. ▪ Public Key and Private Key are used for authentication purposes on the Internet.	a seller of virtual objects that they do not create/own. ▪ Second Life businesses have organised "invitation-only" events and built "group-only" locations, to limit access to avatars that have been authenticated through alternative online and offline means. ▪ Implementation of CAPTCHA-like mechanisms to prevent automated bots from signing up to groups and services within the virtual world.
III. Intellectual Property Theft	▪ Theft of Intellectual Property in (a) Virtual objects, e.g. avatar clothes, virtual building designs, Virtual World applications that include computer codes and scripts. (b) Existing copyrighted materials, e.g. music, video (c) Unauthorised use of real world brand name and trademarks	▪ Creators and owners of visual arts usually restrict still photography to protect their work from unauthorised copying. ▪ The issue of unauthorised sharing of music and video content on the Internet via sharing services like Kazaa, BitTorrent. ▪ The production and sale of pirated goods, e.g. fake Rolex watches.	▪ Dealing with pirated virtual objects. It is possible for creators and owners of virtual objects to alter the settings of a virtual object to prevent copying, resale, modification. However it is still possible for items to be copied through Copybots and simcrash techniques (Reuters 2007e) ▪ Dealing with pirated virtual copies of real products. Many real life brand owners have resorted to building a Second Life presence to control the use of their brand in the Virtual World. However, it is still difficult to ensure that a 3D BMW car made without the authority of BMW is not labelled a BMW. ▪ Difficulty in ensuring that video and audio content streamed in Second Life do not breach existing copyright laws.
IV. Vandalism, Harassment & Stalking	▪ Vandalism and damage to virtual objects and virtual locations. Virtual locations could be defaced ▪ Attacks on avatars through the use of virtual weapons (e.g. push guns, cages).	▪ Online vandalism – websites defaced, hijacked. ▪ Cyber-stalkers on the Internet that use emails, SMS, social networking sites to target victims.	▪ Limiting the freedom of movement of avatars? ▪ Law enforcement agencies may need to take an active role in pursuing stalkers in Virtual Worlds, and make them accountable just as stalkers who have roamed the streets and the Internet.

	▪ Applications and scripted virtual objects could be used to stalk avatars, seize control of avatars.		
V. Defamation & Disparagement	▪ Deception, spreading false and misleading information, rumour mongering. ▪ Libel, defamation and slandering ▪ Disparagement of virtual and real world products.	▪ In the offline environment and on the Internet, consumer affairs advocates take action against sellers that spread false and misleading information ▪ Rumour mongering, product disparagement, slandering libel and defamation on the Internet is treated in much the same way as in the offline environment.	▪ Dealing with negative comments, who is to determine whether comments made in Virtual Worlds are defamatory and libellous? Are there virtual civil actions? It may be much more difficult to pursue a case in Virtual Worlds due to the difficulty in authenticating the identity of avatars. ▪ Balancing freedom of speech and censorship in Virtual Worlds. ▪ Ensuring that culturally sensitive issues and actions that affects the stability of societies are addressed in Virtual Worlds.
VI. Spam & Cybersquatting	▪ Virtual hawkers – avatars that hand out notecards, advertise on group notices and chat channels. ▪ Virtual objects that distribute advertising materials without the expressed consent of virtual location owners. ▪ Avatars and automated bots that squat at virtual locations. The emergence of landbots.	▪ Spam email, physical junk mail and unsolicited advertising materials. ▪ Cyber squatting of web domain, unauthorised hosting of content on computer servers, unauthorised use of Internet bandwidth.	▪ Avatars and organisations operating in Virtual Worlds will need increased awareness on how to exert more control over the virtual world resources they own and operate, to prevent unauthorised use and exploitation. ▪ A major dilemma for Virtual World businesses is – how to encourage genuine visitors and customers, and keep out uninvited hawkers, trouble-makers.
VII. Payment and Transaction Integrity	▪ Transactional security of virtual payments, and the virtual wallet and inventory. ▪ Transactional security of permission request mechanism.	▪ Online retailers rely on different modes and mechanisms to protect the integrity of online payments and transactions. ▪ Ensuring that the transactional mechanism is protected from attacks and exploits.	▪ Implementing a secure and trusted permission request mechanism for payments and transactions. ▪ At present many businesses in Second Life have resorted to 3rd party services like PayPal to facilitate Second Life e-Business. ▪ Financial details (credit card info) of residents have been breached previously.
VIII. Malwares and Computer Virus	▪ The emergence of Copybots, Grey Goo applications and other malicious virtual objects that could crash virtual locations, seize control of avatars, and	▪ Computer virus, Worms, Denial of Service attacks, phishing emails, Trojan horse that carry keyloggers.	▪ Educating avatars on interactions with virtual objects, ensuring that the Virtual World environment could be cleansed and "disinfected".

	disrupt virtual world events.		

Figure 2: Modified version of Lee's (2007) Virtual World Security Threat Matrix

The following discusses a series of major security incidents which have occurred within Second Life. The discussion of the security incident is then mapped to the modified version of Virtual World Security Threat Matrix (Lee 2007) in Figure 2.

Security breach of user details

In September 2006 a hacking attack upon Second Life's database led to the real life personal information of Second Life residents to be breached (BBC 2006a; Lazarus 2006). While much of the data was encrypted, there was a risk of identity theft and financial frauds as a proportion of Second Life residents have registered their credit card details to convert real life currency to Linden Dollars and vice versa. Linden Lab immediately required all users to change passwords after the attack (Fost 2006).

Applicable Threat Dimension(s): I & II

The "Grey Goo" attack

Worm-like malicious virtual objects appeared at various locations on the Second Life Grid in November 2006. The golden ring-shaped virtual objects flooded various Second Life locations by self-replicating. They caused disruption to the Second Life teleportation service, account balance and the rendering of avatar clothing (BBC 2006b; Lemos 2006). The incident was termed a Grey Goo attack as the maliciously coded virtual objects share many similarities with out of control nanotechnology robots that self-replicate and consume all available physical resources. An outright ban on self-replication scripts was not possible as that would limit legitimate use of self-replication for coding virtual objects. Unlike virtual worlds such as There.com, Second Life residents need not submit virtual objects to Linden Lab for approval before the objects could be introduced in the virtual world. Furthermore, Linden Lab encourages Second Life users to create innovative virtual objects, such as virtual plants that grow, multiply, and interact with avatars and virtual environmental elements Although Linden Lab was able to respond to the Grey Goo attack quickly, the incident highlights the vulnerability of the Second Life Grid to attacks by malwares, computer viruses and worms.

Applicable Threat Dimension(s):II, IV, VI & VIII

Griefing attacks

Griefing is an anti-social behaviour that shares many similarities with bullying (Chesney et al. 2007), harassment and vandalism. Griefing is defined as an intentional act that is enjoyed by the attacker, the griefer, and one that affects the victim's experience negatively (Foo and Koivisto 2004). Attackers often take advantage of loopholes and weaknesses in the virtual world mechanism or policies. A griefing attack may target an avatar, an organisation, a virtual location, or a virtual event. In an attack on an avatar, the attacker may use push weapons to displace a victim or override the movement or capabilities of the victim. Griefers have also been known to plant malicious tools and virtual items at virtual locations, or visually vandalise the space by clouding it with large virtual objects that carry disparaging text or graphic. Denial of Service-like griefing attacks occur when a large number of attackers swamp a virtual location or virtual event, generating excessive avatar traffic. Griefers may also attach computing-intensive virtual objects onto their avatars when they visit a virtual location to overload the server that renders the graphics for the virtual location. In December 2006 a real-time CNET interview conducted with Anshe Chung (the avatar of Ailin Graef, a virtual entrepreneur) held in Second Life was severely disrupted by griefers (Terdiman 2006a). In the end the interview had to be moved to an alternative virtual location.

Applicable Threat Dimension(s): IV, V, VI & VIII

Copybot

Another well documented security incident in Second Life relates to the existence of a Copybot application that makes unauthorised copies of virtual objects and avatars (BBC 2006b; Terdiman 2006b). The Copybot application violates Second Life's Terms of Service which stipulates that Second Life residents retain full intellectual property for digital content created in Second Life (2007k). The Copybot application was originally used by developers for debugging purposes, so that developers could import/export digital content into the Virtual World. The application subsequently modified to make unauthorised copies of virtual objects. Although the Copybot application does not operate within the Second Life Grid and does not interfere with Second Life server performance, it rocked the Second Life economy as virtual objects that are usually sold for a price could be copied free of charge. After much protest by residents and businesses, Linden Lab has banned the use of

Copybots and declared its use an infringement of copyright. However, Second Life residents whose virtual objects or avatars have been copied will still need to take individual action against the perpetrator.
Applicable Threat Dimension(s): II & III

Second Life Permission Request Weakness
Second Life residents may allow their avatars to interact with scripted virtual objects in the virtual world. By accepting a permission request emitted by a virtual object, a monetary payment of L$ to the owner of the virtual object may be initiated, or the avatar's movement may be animated. The permission request system could be abused to hide fraudulent and unauthorised monetary transactions, such as charging a price for a virtual object appears visually as a freebie (Second Life 2007l). Once a permission request has been granted, the Second Life resident is not able to pause, cancel or revoke the process.
Applicable Threat Dimension(s): I, II, III, IV, VI, VII & VIII

How are Security Issues Handled in Second Life at present?
The Second Life environment is a complex environment and Linden Lab has identified security as being a key issue. At this point, it is important to evaluate the existing mechanism for addressing security issues in Second Life. Linden Lab has identify security as being (Second Life, 2007m):

> *If an issue poses any of the following threats to Second Life, its Residents or content, then it is an exploit and should be reported:*
>
> - *exposes real life resident identity without consent*
> - *destroys content*
> - *permits unauthorized access to Second Life/Linden Lab resources*
> - *compromises a client or server host subjecting it to remote control*

The security configuration of Second locations are determined by the settings of the location or island. For instance, island owners can make an island private and limit access to a cohort of residents. In this way, a private island operates much like an Intranet that runs inside an organisational firewall. However, a key difference lies in the fact that the island is still hosted on a Linden Lab computer server rather than a private computer server owned by a business or resident. At present, the only legally enforceable contract between Linden Lab and users of Second Life is Second Life's Terms of Service. Avatars that breach the Terms of Service may be banned from Second Life.

CONCLUSION

Virtual Worlds like Second Life, both as a concept and a technological platform, have a huge potential for the future. More and more organisations will offer their services and products to the residents of second life. However, one of the main challenges facing Second Life at present is that security issues in Virtual Worlds transcends the boundary between the real and virtual worlds. Hence, only a limited set of technical tools may be used to secure the Second Life system, especially with the emphasis by Linden Lab to have minimal intervention in the virtual world environment. Several security issues within Second Life will need to be dealt with through a social approach, such as educating avatars on virtual world ethics.

The existence of unlawful activities in Virtual Worlds, such as gambling and betting, have drawn attention from real world law enforcement agencies (Times 2007). There is also a concern that security incidents in Virtual Worlds may also lead to unrest in Virtual Worlds, and produce consequences that extend to the realms of the real world, e.g. real world protests, frauds, identity theft and stalking. It would be detrimental for Virtual Worlds like Second Life if users and businesses which have invested resources withdraw their support and reduce their participation. Further complicating the issue is the fact that security threats in Virtual Worlds will continue to evolve as more and more real world activities and phenomena are transfused, translated and extended into Virtual Worlds.

This paper contributes to practice and research by providing a broad overview of security issues in Second Life and other Virtual Worlds, and raises awareness among Second Life businesses and residents on emerging security issues. For Second Life residents and businesses, the challenge lies in staying ahead of these security threats, in particular those related to the social networking phenomena, and identifying possible social and technical solutions for overcoming the problem.

REFERENCES

Barbagli, F., Salisbury K and Devengenzo R (2004) Sensor Review, Vol 24, Issue 1, Emerald Press, UK.

BBC (2006a) "Security Row Upsets Second Lifers" BBC News, URL: http://news.bbc.co.uk/1/hi/technology/5365148.stm [Accessed 31 October 2007]

BBC (2006b) "Worm Attacks Second Life World" BBC News, URL: http://news.bbc.co.uk/1/hi/technology/6164806.stm [Accessed 13 September 2007].

Bray, D., and Konsynski, B. (2007) "Virtual Worlds, Virtual Economies, Virtual Institutions" Emory University, URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962501 [Accessed 29 October 2007]

Chesney, T., Coyne, I., Logan, B., and Madden, N. (2007) "A Design for Researching Virtual Worlds – Opportunities and Limitations" Proceedings of the European Conference on Information Systems, St. Galen, Switzerland.

Courier Mail (2007) "Sweden opens Second Life embassy", 31st May 2007.

Foo, C. Y., and Koivisto, E. M. I. (2004) "Defining Grief Play in MMORPGs: Player and Developer Perceptions" Proceedings of the International Conference on Advances in Computer Entertainment Technology, Singapore.

Fost, D. (2006) "Second Life hack attack causes second-guessing" San Francisco Chronicle, 12 September 2006, URL: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/09/12/BUGQ6L3K081.DTL [Accessed 29 October 2007]

Harvard Law School (2006) "Berkman Center and Harvard Extension School to Offer First University Course through Second Life, a 3-D Virtual Environment" URL: http://cyber.law.harvard.edu/home/newsroom/pressreleases/harvard_extention_school_to_offer_first_university_course_through_second_life [Accessed 1 August 2007]

Hemp, P. (2006) "Avatar-based Marketing" Harvard Business Review, 84 (6), pp. 48-57.

Hof, R. (2006) "My Virtual Life" Business Week, 1 May 2006, URL: http://www.businessweek.com/magazine/content/06_18/b3982001.htm [Accessed 29 October 2007]

Hutcheon, S (2007a) IBM expands virtual world presence, The Age, 24th August, 2007.

Hutcheon, S (2007b) Jitters in Second Life as bank shuts doors, Sydney Morning Herald, 10th August, 2007.

Guardian (2007) "Exploding pigs and volleys of gunfire as Le Pen opens HQ in virtual world" URL: http://www.guardian.co.uk/technology/2007/jan/20/news.france/print [Accessed 11 September 2007].

Lamont, I. (2007) "Harvard's virtual education experiment in Second Life", URL: http://www.computerworld.com/blogs/node/5553 [Accessed 12 September 2007]

Lazarus, D. (2006), "Real fear in virtual world", San Francisco Chronicle, 15th September.

Lee, C. Y. (2007) "Virtual World Security" Work in progress paper, School of Information Systems, Deakin University, Australia.

Lemos, R. (2006) "Second life plagued by 'grey goo' attack" The Register, 24 November 2006, URL: http://www.theregister.co.uk/2006/11/24/secondlife_greygoo_attack/ [Accessed 29 October 2007]

Ohio State University (2007) Ohio University Second Life Campus, URL: http://vital.cs.ohiou.edu/vitalwiki/index.php/Ohio_University_sims [Accessed 10th August, 2007].

Reuters (2007a) "HBO buys film made in Second Life" 4 September 2007, URL: http://www.reuters.com/article/technologyNews/idUSN0444783420070904 [Accessed 5 September 2007]

Reuters (2007b) "Congressional Democrats' agenda gets SL stage" 2 January 2007, URL: http://secondlife.reuters.com/stories/2007/01/02/congressional-democrats-agenda-gets-sl-stage/?&src=010407_1334_ARTICLE_PROMO_also_on_reuters [Accessed 1 August 2007]

Reuters (2007c) "Rosedale opens SLCC with apology for bugs", 25 August 2007, URL: http://secondlife.reuters.com/stories/2007/08/25/rosedale-opens-slcc-with-apology-for-bugs/ [Accessed 1 September 2007].

Reuters (2007d) "Rival grids threaten Linden's monopoly on SL technology" 6 September 2007, URL: http://secondlife.reuters.com/stories/2007/09/06/rival-grids-threaten-lindens-monopoly-on-sl-technology/ [Accessed 17 September 2007].

Reuters (2007e) "Eros lawyers ID 'John Doe' avatar; Youth denies he's Catteneo" 25 October 2007, URL: http://secondlife.reuters.com/stories/2007/10/25/eros-lawyers-id-john-doe-avatar-youth-denies-hes-catteneo/ [Accessed 29 October 2007]

Rose, F. (2007) "How Madison Avenue Is Wasting Millions on a Deserted Second Life" Wired Magazine, Issue 15.08, URL: http://www.wired.com/print/techbiz/media/magazine/15-08/ff_sheep, [Accessed 1 August 2007].

Salomon, M. (2007) "Business in Second Life: An Introduction" Swinburne University of Technology, Australia, URL: http://smartinternet.com.au/ArticleDocuments/121/Business-in-Second-Life-May-2007.pdf.aspx [Accessed 1 August 2007]

Second Life (2007a) What is Second Life?, URL: http://secondlife.com/whatis/ [Accessed 15th August, 2007].

Second Life (2007b) Economy, URL: http://secondlife.com/whatis/economy.php [Accessed 15th August, 2007].

Second Life (2007c) Economic Statistics, URL: http://secondlife.com/whatis/economy_stats.php [Accessed 15th August, 2007].

Second Life (2007d) Economic Statistics, URL: http://secondlife.com/whatis/economy_stats.php [Accessed 15th August, 2007].

Second Life (2007e) Quality Assurance Portal, URL: http://wiki.secondlife.com/wiki/QA_Portal [Accessed 15th August, 2007].

Second Life (2007f) What Is Our Antivirus Protection Policy, URL: h http://wiki.secondlife.com/wiki/What_Is_Our_Antivirus_Protection_Policy [Accessed 15th August, 2007].

Second Life (2007j) Terms of Service, URL: http://secondlife.com/corporate/tos.php [Accessed 16 September 2007].

Second Life (2007k) Terms of Service, URL: http://secondlife.com/whatis/ip_rights.php [Accessed 16 September 2007]

Second Life (2007l) "LlRequestPermissions(llGetOwner(), PERMISSION REFUND)" URL: http://wiki.secondlife.com/wiki/LlRequestPermissions(llGetOwner(),_PERMISSION_REFUND)%3B [Accessed 1 November 2007]

Second Life (2007m) Security Issues, URL: http://wiki.secondlife.com/wiki/Security_issues [Accessed 15th August, 2007].

Terdiman, D. (2006a) "Virtual Magnate Shares Secrets of Success" ZDNET, 20 December 2006, URL: http://news.zdnet.com/2008-9588-6144967.html [Accessed 1 August 2007].

Terdiman, D. (2006b) "'Second Life' Faces Threat to its Virtual Economy" CNET, 15 November 2006, URL: http://www.news.com/Second-Life-faces-threat-to-its-virtual-economy/2100-1043_3-6135699.html?tag=newsmap [Accessed 31 October 2007].

Times (2007) "FBI goes virtual to investigate SecondLife casinos" 4 April 2007, URL http://business.timesonline.co.uk/tol/business/industry_sectors/leisure/article1613283.ece [Accessed 1 August 2007].

COPYRIGHT

Lee & Warren © 2007. The author/s assign the We-B Centre & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to the We-B Centre & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.