Understanding Security Threats in Virtual Worlds

Chia Yao Lee
Deakin University, chia.lee@deakin.edu.au

Recommended Citation
http://aisel.aisnet.org/amcis2009/466

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Understanding Security Threats in Virtual Worlds

Chia Yao Lee
School of Information Systems,
Deakin University,
Melbourne, Australia
chia.lee@deakin.edu.au

ABSTRACT
The influx of Fortune 500 companies like IBM, Toyota and Starwood Hotels into the virtual world of Second Life has generated much publicity in 2006 and 2007. The virtual world landscape has changed substantially since. Many early adopters have abandoned virtual worlds, and the number of security-related incidents in virtual worlds has risen substantially. This paper discusses key security threats in virtual worlds, and highlights the need for users and stakeholders to better understand these threats in order to manage them more effectively. The issue of managing security threats in virtual worlds is especially important in ensuring that virtual worlds remain a friendly environment to thriving online communities and e-business; and represent an environment whereby the interests of various stakeholders are protected and upheld. The paper contributes to practice and research by (i) raising security awareness among virtual world users and stakeholders, and (ii) prescribing a systematic approach for analyzing the nature and implication of security threats in virtual worlds.

Keywords
Virtual worlds, security threats, computer ethics

INTRODUCTION
Virtual worlds such as Second Life, ActiveWorlds and There have generated substantial press coverage in 2006 and 2007 due to the influx of Fortune 500 companies (Reuters 2006). In 2006 IBM announced that it had plans to invest over US$100 million in virtual world-related activities over a period of two years (IBM 2006). IBM has over a thousand employees who are registered users of Linden Lab’s Second Life. IBM employees use virtual worlds to host business meetings and conferences with its clients. IBM also has integrated virtual world capabilities within its Lotus SameTime IM product. Prior to the official debut of their Aloft Hotels product, Starwood Hotels created a virtual replica of an Aloft Hotel in Second Life to enable potential customers to tour and experience the new product (Reena 2006). Visitors to the virtual hotel could interact with features of the hotels, and visualize its interior décor and poolside architectural design. The exercise enabled Starwood Hotels to gain valuable input directly from potential customers (Reena 2006). Such events gave credence to virtual worlds among members of the business community and propelled virtual worlds into the boardrooms of marketing firms and multinational companies.

2006 also marked the emergence of security threats in virtual worlds. In November that year, the virtual world of Second Life experienced a Grey Goo attack (Lemos 2006). Self-replicating virtual objects flooded the virtual environment, causing disruptions to the virtual environment and its users (Lemos 2006). Apart from causing disruptions to users, the Grey Goo attack has nonetheless provided a proof of concept for malicious worm-like computer virus in virtual worlds. In December that year, an in-world (i.e. held within the virtual world) interview with Anshe Chung, the avatar of the successful virtual world entrepreneur Ailin Graef, was disrupted by griefers (Terdiman 2006). Whilst the grieving attack was no more a nuisance than a serious security breach, it has demonstrated the vulnerability of virtual worlds to online protests and grieving attacks. Sustained grieving attacks may produce effects which are similar to Denial of Service (DOS) attacks. Other incidents relating to the emergence of pyramid and ponzi scams in virtual worlds, unregulated virtual banking and gambling, and simulated illegal activities in virtual worlds have further raised concerns among practitioners, law enforcement agencies, government regulators and legislators (Reuters 2008a; Semuels 2008; Sipress 2007). Such was the extent of concern among American legislators that Philip Rosedale, the founder of Second Life, was called before a U.S. senate subcommittee to discuss security and ethical issues in virtual worlds (Reuters 2008b). In Rosedale’s testimony he acknowledged the potential
misuse of virtual worlds for gambling, money laundering, and the need to address child safety and virtual banking issues in virtual worlds (Rosedale 2008). Expressing similar concerns, the European Network and Information Security Agency (ENISA) produced a report in November 2008 which highlighted 14 specific security risks associated with virtual worlds (ENISA 2008).

As more aspects of our modern society are replicated, simulated, extended into, and experienced within virtual worlds, there is an increased urgency to address security threats in virtual worlds. This is to ensure that virtual world security threats are managed effectively, and to ensure that they do not produce consequences that spillover into the real world. The research questions that underpin the paper ask

“What are the emerging security threats in Virtual Worlds?” and

“How should stakeholders manage security threats in Virtual Worlds?”

In seeking to address the above questions, the paper discusses a systematic approach for analyzing the nature of security threats in virtual worlds and their implication on users and stakeholders. Intended as a discussion paper, the paper proposes several modifications to Lee and Warren’s Virtual World Security Threat Matrix (2007). The modifications will extend the coverage of the Lee and Warren’s framework, and adapt the framework for analyzing the nature, implication and severity of virtual world security threats. Subsequent studies have been planned to test the validity of the modified framework, and use the modified framework to generate other testable propositions, however these are beyond the scope of the current paper. Upon validation, it is hoped that practitioners will find the modified framework useful for prescribing a systematic approach for managing security threats in virtual worlds.

The paper contributes to practice and research by (i) raising security awareness among virtual world users and stakeholders, and (ii) providing insight into the nature and implication of different security threats in virtual worlds. The research team has selected the virtual world of Second Life as the main platform for the present discussion due to the diversity of social and economic activities that take place within Second Life, and Second Life’s motto that encourages users and stakeholders to take an active part in developing and managing the virtual world.

LITERATURE REVIEW

What are Virtual Worlds?

Virtual worlds are Multi-User Virtual Environments (MUVEs) that enable users to interact with each other through synthetic, 3D graphical environments that are hosted on networked computers. Virtual worlds share many similarities with existing telecommunication technologies and Internet applications such as instant messaging, Voice over Internet Protocol (VoIP), social networking, networked computer games and Wikis. However, virtual worlds combine these applications on a platform that has the additional support for synthetic 3D graphical environments. Virtual worlds possess several unique attributes that distinguish them from early Virtual Reality (VR) applications (Schroeder 2008). These attributes include persistent existence, real-time synchronization, user-contributed content (Bell 2008), and the ability to integrate with existing Internet services such as emails, video and audio-streaming.

The synthetic 3D graphical environments for virtual worlds could be accessed through a browser-like client application called the Viewer. Specialized audio-visual and spatial equipments are not required for accessing virtual worlds. The content and activities within virtual worlds may be modeled on real life, or be totally imaginary. Hence, virtual worlds are sometimes referred to as alternative realities and metaverses. When in-world events are synchronized with events in the real world, they are termed mixed reality events. These may include conferences, seminars, and meetings which are streamed into virtual worlds, enabling in-world participants to interact with real world participants through text and audio chats. Attendees of the World Economic Forum in 2007 and 2008 interacted with Second Life users through sessions streamed into Second Life (WEF 2007).

Although many online computer games like the World of Warcraft and The Sims Online also employ synthetic 3D graphical environments, not all virtual worlds have been designed to operate as a game even though they may have the ability to support role-play and other gaming activities. The Sims Online and the World of Warcraft belong to the genre of computer games known as Massively Multi-user Online Role Playing Games (MMORPGs). MMORPGs have game-specific objectives, rules and regulations which are pre-determined by game developers, and mechanisms that reward or penalize users for their achievements or actions. In comparison, virtual worlds like Second Life and There are socially-oriented; they do not have specific themes or game objectives, and often allow users to take the initiative in determining the types of activities which should take place within the virtual environment.
A majority of virtual worlds support Real Money Trading, whereby virtual currencies within a virtual world could be converted into real world currencies and vice versa (Dibbell 2008). Virtual currencies could be exchanged for real world currencies through foreign exchange-like mechanisms. The currency conversion rate is primarily determined by the demand and supply for the virtual currency, and also the occasional intervention by the virtual world’s owner or developer. The existence of virtual currencies underpins the existence of in-world economies in several virtual worlds (Bray and Konsynski 2008). Users could trade anything from avatar clothing and accessories to virtual land and real estate. Several real world companies have developed in-world applications that interact with their World Wide Web applications. These applications enable users to access their real world products through virtual worlds, for example, Vodafone’s Inside Out application enable Second Life users to send text messages from within virtual worlds to real world mobile phones, and pay for the services in Linden Dollars, Second Life’s virtual currency (SecondLifeInsider 2007). On average, more than US$1 million in economic activities take place within Second Life’s in-world economy each day.

Existing research on virtual worlds straddle several academic disciplines, ranging from law (Balkin 2004; Boonk and Lodder 2007; Grimmelmann 2004) and medicine (Lofgren and Fefferman 2007) to economics (Bray and Konsynski 2008) and computer science (Friedman et al. 2007). The diversity of these disciplines suggests increasing interest among researchers in different fields, as well as the breadth of opportunities presented by virtual worlds to practitioners in these disciplines. Virtual worlds have gained substantial interest among e-business and information systems researchers, for instance, Sharp and Rowe (2006) discussed possibilities for new business models and markets to form in virtual worlds. They also discussed how these new virtual world business models may shape the future of the entertainment industry. Bray and Konsynski (2008) discussed issues such as the economics of virtual world activities, and the formation of virtual institutions and social mechanisms for governing virtual worlds. Adopting a more technical perspective, Myles and Nusser (2006) studied various techniques for developers and content developers for protecting content and intellectual property in virtual worlds and computer games. Computer security practitioners and anti-virus software firms like McAfee and Kapersky Lab have also acknowledged the possibility of criminal elements taking advantage of the often lawless virtual world environment to carry out attacks on unsuspecting virtual world users (Kapersky 2008; Muttik 2008). The existence of virtual currencies and Real Money Trading increases the risk of virtual world users falling for online scams and computer attacks. Elliot and Kruck (2008) discussed the emergence of various forms of financial frauds and scams in virtual worlds like pyramid and Ponzi schemes.

Activities and Events within Virtual Worlds

In order to better comprehend the nature of security threats and their implications, one has to understand the wide range of social and economic activities which take place within virtual worlds. In broad terms these activities can be categorized as (a) business and commerce, (b) education and training, (c) charity and non-profit, and (d) politics and government.

(a) Business and Commerce

Substantial interest in leveraging virtual worlds for business and commerce came from marketing firms and large multinational companies. These real world companies had plans to transplant existing real world business models into virtual worlds, and target the virtual world users using the same methods used in the real world. Many marketing firms helped clients establish virtual branches, host virtual product launches and press conferences, while others sought to plaster the virtual environment with poster-like advertisements that contain hyperlinks to websites on the World Wide Web. Such marketing activities were effective in generating short-term publicity, but as they seldom involve employees, suppliers and customers, the activities did not lead to long-term, large scale adoption of virtual worlds.

More successful virtual world adopters such as IBM and Cisco focused on using virtual worlds to host business meetings and conferences with customers and trading partners (Wagner 2007). Employees, suppliers and customers interact closely in virtual worlds, collaborating on projects by using the 3D graphical platform to visualize data and design products. Real world companies which have been more successful in virtual worlds have largely concentrated on leveraging the multi-user collaborative environment of virtual worlds, and exploit their capability in supporting 3D simulation of environments and data visualization.

A significant proportion of business and commercial activities in virtual worlds can be attributed to in-world companies that serve the needs and requirements of virtual world users. These in-world companies developed virtual furniture and appliances, scripted virtual tools, avatar clothing, as well as provide services to help customers enhance their virtual world experience. Simulation and interactive role-play games have also been used by businesses to both foster a community of fans and supporters, as well as for generating in-world revenues from the sale of virtual admissions and virtual accessories for games.

(b) Education and Training
Universities and educational institutions have also embraced virtual worlds warmly. The synthetic 3D graphical environments provided by virtual worlds are particularly useful for hosting distance education, simulation of learning environments, visualization of models, as well as classroom activities that require close interaction among students. Leading universities in the world, as well as consortia of universities and educational institutions are currently at the forefront of using virtual worlds for teaching and learning, and as a platform for academic research. Virtual worlds have been used as a teaching and learning platform for academic disciplines as diverse as music and fine arts, business and law, information systems, engineering, computer science, architecture, medicine and nursing.

(c) Charity and Non-Profit

The charity and non-profit sector has also adopted virtual worlds widely to support and complement their real world operations. The American Cancer Society hosted a series of Relay for Life charity events within Second Life. Its 2007 in-world event raised donations totaling more than US$118,000 (ACS 2007). A virtual Camp Darfur was created by human rights advocates to highlight the suffering of Darfur residents (SecondLifeInsider 2006). In December 2008, the US Holocaust Museum launched a virtualized version of the physical Holocaust Museum to commemorate the 70th anniversary of the Holocaust, and to raise awareness for the historical event (USHMM 2009). Virtual worlds represent a useful and effective channel for promoting charity and non-profit causes as they support on-demand video and audio streaming, as well as the ability to simulate immersive 3D environments.

(d) Politics and Government

Politicians and their supporters have also been at the forefront of using virtual worlds for lobbying and campaigning. Political campaigns for parties involved in the French national election in 2007 used Second Life to reach out to in-world supporters. These virtual political campaigns have even led to in-world protests and chaos when supporters and opponents of Jean-Marie Le Pen, a presidential candidate, used virtual weapons to attack each other (Moore 2007). In the USA, early campaigning activities by supporters of presidential hopefuls like Hillary Clinton and Barack Obama have also taken place within virtual worlds (Lawton 2008). On the other hand, the Swedish government has established a virtual embassy within Second Life to promote tourism and business networking (Simmons 2007).

The Growing Importance of Virtual World Security

There is little doubt that various aspects of our modern society have been extended into virtual worlds. In-world events and activities closely mimic their real life counterparts, and are no longer detached from real world events. Of great concern to virtual world developers, government regulatory bodies and law enforcement agencies is the need to ensure that criminal activities and anti-social behaviors do not spread unchecked in virtual worlds.

In recent times real world courtrooms have been used to deal with criminal and anti-social activities within virtual worlds. In the Netherlands, a teenage user of the Runescape virtual world had been sentenced to jail for forcing his victim in the virtual world to handover virtual money and property (Feldmann 2008). The landmark lawsuit initiated by Kevin Alderman against avatar Volkov Catteneo demonstrated how an infringement of copyright within virtual worlds could be pursued through the real world justice system (Richards 2007). The Alderman vs. Catteneo case had also highlighted the challenges involved in tracking down and pursuing lawbreaking avatars. It has come as no surprise to many observers that Linden Lab shut down and banned virtual gambling operators in Second Life because such activities were considered unlawful in certain legal jurisdictions if they were not licensed. A ban on unlicensed virtual banks in Second Life was put in place after the failure of Ginko Financial (Hutcheon 2007), a self-proclaimed virtual bank in Second Life which had more similarities with a Ponzi scheme than a real world banking institution.

The severity of security incidents in virtual worlds highlights the lack of governance and regulation of virtual worlds. It also highlights the risk of criminal elements taking advantage of the lawlessness of virtual worlds to target unsuspecting virtual world users by initiating phishing attacks, computer worm attacks and other forms of malicious activities. Realizing the seriousness of security and ethical issues in virtual worlds, IBM has introduced the “Virtual Worlds Guidelines” for its employees in 2007 (IBM 2007). The above examples suggest the real need for virtual world users and stakeholders to better understand and manage security threats in virtual worlds.

authentication and identity theft, (iv) vandalism, harassment and stalking, (vi) spam and cybersquatting, and (viii) malwares and computer viruses. The framework aids the formulation of technical countermeasures, as well as the formulation of policies and strategies for addressing security threats in virtual worlds.

METHODOLOGY

As a discussion paper, the current paper aims to highlight the severity of security threats in virtual worlds, and implication of these threats on activities and events within virtual worlds and in the real world. Further studies have been planned to test the validity of the modified Virtual World Security Threat Matrix under different circumstances. Immediate plans are in place for focus group workshops to be conducted with adopters of virtual worlds to gain a deeper insight into stakeholder perception of security threats in virtual worlds, and their knowledge and level of awareness of these threats. It is hoped that data collected from the focus group workshops will help validate the modified framework, and provide an opportunity to generate testable propositions for future quantitative work in the area. Other virtual world security frameworks, such as the one by ENISA (2008), have not been used as they were more akin to a list of security threats, and are not as suited for analyzing the multi-dimensional nature security threats.

DISCUSSION

Current literature on security threats in virtual worlds have largely concentrated on disruptive griefing attacks within virtual worlds (Exchange 2007; Terdiman 2006). Although concerns with how avatars could inflict disruptions on other avatars are especially captivating when these actions are visualized in 3D, of equal importance to researchers and practitioners is the emergence of fraudulent activities and scams in virtual worlds. Virtual theft for instance, is another threat which is unique in virtual worlds due to the ability for virtual real estate, virtual possessions and virtual currencies to be stolen and traded fraudulently.

Focusing on gaming-type virtual worlds, ENISA has emphasized the current lack of online dispute resolution in virtual worlds. There are also concerns regarding the use of “Gold Farming” whereby users engage third parties to perform tasks and activities to cheat other users (Dibbell 2007). Although using Gold Farming to gain an unfair advantage is no different to employing physical sweatshops in third world countries, of great concern to virtual world users is the rise of online syndicates that aim to gain an unfair advantage over other users, and provide these services at a price, to whoever is willing to pay. Gaming-themed virtual worlds such as the World of Warcraft have explicit regulations that outlaw Gold Farming.

To further expand the coverage of Lee and Warren’s framework, the current paper introduces 2 additional dimensions of security threats – (ix) Frauds and Scams, and (x) Simulated virtual crime, as illustrated in Table 1.

(ix) Frauds and Scams

An expansion of the Lee and Warren (2007) framework to include Frauds and Scams was motivated by the ban imposed by Linden Lab in 2008 on unlicensed banking operations (Second Life 2008), and the ban on various forms of land-griefing and landbots which artificially manipulate the price of virtual real estate (Reuters 2007). The new threats dimensions have become possible because virtual worlds support scripted virtual applications and bots, i.e. remote-controlled artificial intelligence-like virtual objects, which may scour the virtual environment and compete against human-controlled avatars in land purchases. The Real Money Trading capability of virtual worlds has made the virtual worlds vulnerable to pyramid and ponzi scams. Virtual currencies may be channeled out from the virtual environment once a victim is attacked. Although such scams within virtual worlds may not involve large volume of money, a more worrying concern lies in syndicates that use virtual worlds to conduct large scale frauds and money laundering. A collection of numerous micro transactions between avatars, and subsequent conversion of virtual currencies into real world currencies may be used to cover the tracks of money laundering. This has been cited as one of the underlying reasons for Linden Lab to ban unlicensed virtual banking operations as virtual banks could be easily exploited for money laundering.

The frauds and scams category also includes Gold Farming because virtual world users may employ third parties to perform certain tasks in exchange for real world currencies and in turn enhance the well-being and social status of their avatars. Such actions short-circuit existing rules and conditions within virtual worlds, and have become a concern in virtual world users and developers. Gold farming activities enable users to make redundant, if not cheat the system put in place for generating virtual wealth and value.
(x) Simulated Virtual Crime

The other new dimension added to Lee and Warren’s Virtual World Security Threat Matrix is labeled Simulated Virtual Crime. It relates to how virtual world users may use the virtual environment to replicate a real life criminal activity, e.g. kidnap or rape of an avatar, or age-play, whereby users manipulate avatars that resemble underage minors to perform sexual acts. Simulated virtual crime and age-play are banned in several European countries (Lynn 2007). Although simulated virtual crime may not produce direct effects on innocent unsuspecting victims if the activity was performed among consenting adult users of virtual worlds, they are a worrying concern for law enforcement agencies and security researchers as these simulations may become part of a training process for recruiting potential victims, or if the simulated activities could be re-enacted in the real world. Virtual worlds may become a training ground for criminal activities, and enable criminal elements to perfect skills for breaking the law in the real world.

In order to provide an in-depth analysis of each of the ten security threat dimension, the Lee and Warren (2007) framework has also been expanded to incorporate two distinct views on the 10 virtual world security threat dimensions. These two views are (a) the Social Engineering aspect, and (b) the Technical aspect.

The Social Engineering Aspect of Virtual World Security Threats

The Social Engineering aspect of security threats illustrates how security threats in virtual worlds may exploit the social trust mechanism between users to facilitate security breaches. Due to the heavy reliance of virtual worlds on social networking and social interactions between users, it is becoming apparent that emerging security threats in virtual worlds could take advantage of the social engineering and target specific weaknesses that exploit the gullibility of users. Security threats that take the form of phishing attacks, cyber-stalking and online bullying represent this new breed of threats which take advantage of the gullibility of users. In virtual worlds, examples of social engineering-motivated attacks also include the posting of malwares that masquerade as freebies, and the posting of teleport phishing virtual destinations in group messages.

The Technical Aspect of Virtual World Security Threats

Security threats in virtual worlds could also be viewed through a technical perspective. Several security threats in virtual worlds exploit the technical weaknesses of the virtual world platforms, e.g. servers which used to store sensitive user information may not be secured against worms and attacks. The security of virtual environments and the integrity of virtual objects may also be targeted by malwares and bots that scan for weaknesses. For example, data scraping bots may probe virtual environments to look for unsecured property, and hijack these unsecured resources. They could also scan the ownership attributes of virtual objects and implant virtual eavesdropping devices which then monitor the activity and conversation of avatars without their knowledge.

The transaction authorization mechanism in virtual worlds represents a major source of weakness. Transaction mechanisms in virtual worlds do not have the same level of security as online banking systems. The lack of third party-verified certificates, private and public key infrastructure in virtual worlds also greatly diminishes the ability for users to authenticate the veracity and accuracy of information, and distinguish genuine virtual products from unauthorized copies. The problem is further complicated by a lack of computer forensic tools for virtual world users and stakeholders to trace the trail unlawful virtual activities, so as to safeguard themselves against uninvited bots, unsolicited marketers, and other forms of criminal activities.
<table>
<thead>
<tr>
<th>Security Threat Dimension</th>
<th>Description</th>
<th>Social Engineering Aspect</th>
<th>Technical Aspect</th>
</tr>
</thead>
<tbody>
<tr>
<td>(i) Privacy and Confidentiality</td>
<td>Breach of information and data integrity due to unauthorized monitoring and recording of avatar conversation and activities, which may lead to the exposure of personal information and behavioral data.</td>
<td>Much like social networking applications Facebook and MySpace, virtual worlds enable users to create contact lists and enable contacts to view their personal information, e.g. association with groups, online activities. Of particular concern is unauthorized monitoring of avatar activities and conversation, which may lead to exposure of personal information and data.</td>
<td>Due to the way many virtual world users configure their avatars to contain limited links to their real life personal information, concerns regarding the direct leak of personal information is less of a concern. Of a greater concern is the breach of security in computer servers that store user information.</td>
</tr>
<tr>
<td>(ii) Authentication and Identity Theft</td>
<td>Verification of avatar identity which may be faked or reverse-engineered due to weak mechanisms for authentication and trust-building</td>
<td>Authentication and Identity Theft issues in virtual worlds could also exploit social networks in virtual worlds, and the gullibility of users.</td>
<td>Existing authentication mechanisms in virtual worlds are weak, and the ability for users to create avatars anonymously makes authentication difficult, and identity theft rife in virtual worlds.</td>
</tr>
<tr>
<td>(iii) Intellectual Property Theft</td>
<td>Unauthorized reproduction and use of copyrighted and protected intellectual property, e.g. unauthorized use of trademark and brandnames.</td>
<td>Intellectual property theft in virtual worlds has not exploited social engineering weaknesses.</td>
<td>Intellectual property infringement in virtual worlds can be largely attributed to a lack of effective enforcement and dispute resolution mechanism. As such, the costs for owners of IP to pursue unauthorized use of their IP often exceed the level of penalty.</td>
</tr>
<tr>
<td>(iv) Vandalism, Harassment and Stalking</td>
<td>Cyber-bullying and harassment that restrict the freedom of virtual world users. These may include damaging virtual real estate and property.</td>
<td>Online harassment and cyber-bullying in virtual worlds may exploit social engineering weaknesses, and are difficult to deal with since there is a lack of computer forensic tools for users.</td>
<td>Online harassment and cyber-bullying in virtual worlds are mostly a social issue, but there is a potential for vandals and stalkers to take advantage of weak mechanisms that protect the freedom of movement of avatars in virtual worlds.</td>
</tr>
<tr>
<td>(v) Defamation and Disparagement</td>
<td>Deception, spreading of false and misleading information that may lead to damages to reputation and character.</td>
<td>Virtual threats and disparaging remarks may exploit social engineering weaknesses in virtual worlds.</td>
<td>Not applicable.</td>
</tr>
</tbody>
</table>
(vi) Spam and Cybersquatting

Unauthorized use of virtual resources, unsolicited communication between avatars.

Spamming in virtual worlds and unsolicited communication between avatars normally exploit the social context of virtual world activities.

The complexity associated with security virtual property and real estate against virtual squatters may be overcome by a deeper understanding of existing security tools and settings.

(vii) Payment and Transaction Integrity

Transactional integrity of virtual payments and inventory.

Not applicable.

Current mechanisms for payment and transaction authorization are relatively weak compared to online banking systems.

(viii) Malwares and Computer Viruses

Scripted bots and malicious applications that may seize control of avatars and virtual resources.

Due to the possibility of hosting AI-driven bots, and malwares that perform pre-determined tasks, it has become possible for malwares and scripted bots to exploit social engineering weaknesses in virtual worlds.

Whilst virtual worlds support a wide range of automated bots, the lack of policy and rules regulating bots continue to make users vulnerable to sophisticated bots that appear like human-controlled ones.

(ix) Frauds and Scams

Fraudulent financial activities that take advantage of unwary users, e.g. pyramid and ponzi schemes.

The ability to replicate real life business models has made it possible for perpetrators to target gullible users in virtual worlds.

Existing data-mining methods may be used to monitor financial transactions in virtual worlds to spot fraudulent transactions and scams.

(x) Simulated Virtual Crime

Simulation of anti-social and illegal activities such as age-play, virtual prostitution, and unlicensed gambling.

The virtual environment is well-suited for simulation of virtual criminal activities, e.g. abuse of minors. The social engineering aspect of virtual worlds could be easily exploited as there is a lack of policing and law enforcement within virtual worlds.

There is a lack of automated mechanisms for monitoring “acceptable” and “unacceptable” activities in virtual worlds. Hence regulation of simulated virtual crime will require greater input in-world users.

Table 1. A modified version of Lee and Warren’s (2007) Virtual World Security Threat Matrix

CONCLUSION

Security threats have so far created disturbances, disruptions and chaos within virtual worlds. Practitioners are especially concerned with securing virtual worlds to ensure that disruptions and chaos do not spill over into the real world. Another security concern relates to the extent to which real life legal systems extend into virtual worlds. Increasingly we are seeing the real life legal system being used to settle disputes in virtual worlds. For instance, the dispute over the theft a prized virtual sword has led to the murder of a user in real life in China in 2005. The murderer was subsequently sentenced to life imprisonment (BBC 2005). In the USA, the breakdown of a virtual relationship between two users in Second Life had led to the attempted kidnapping of a user in real life (ABC 2008). A dispute over intellectual property theft in virtual worlds has led to legal proceedings in a real life court (Davis 2007). Hence, security threats that originate from virtual worlds may appear “virtual” for now but they tend to have a real impact on virtual world users and stakeholders. This is not surprising given the large number of virtual world users who spend a substantial part of their lives immersed in virtual worlds, living an extension of their real life in the synthetic environments of virtual worlds.
The modified Virtual World Security Threat Matrix presents a systematic approach for gaining a deeper understanding of security threats in virtual worlds. The framework helps users and stakeholders identify and counter current and emerging threats. The introduction of the social engineering and technical aspects of security threats enables one to analyze the nature and severity of security threats in virtual worlds, and formulate appropriate strategies to counter the threats. The modified framework helps corporate users map the implications of security threats in virtual worlds, and develop policies and protocols to enhance the governance of social and economic activities in virtual worlds.

For practitioners and corporate users, the paper emphasizes the urgency for securing virtual environments. Policies and governance structures will be needed to ensure that employees and trading partners are protected from untoward activities in virtual worlds, and to ensure that corporate intellectual and virtual properties in virtual worlds are safe from unauthorized use. For policymakers, regulators and legislators, the paper has discussed how security threats in virtual worlds present new challenges that require existing legislations and regulations to be modified to cover activities in virtual worlds. Technical solutions to overcome security threats in virtual worlds may provide a temporary relief, but in the longer-term virtual world security threats will have to be addressed through education and by increasing user awareness, cultivating community values, and building a culture that discourages unethical and opportunistic behavior in virtual worlds.

REFERENCES


