Exploring Security Risks in Virtual Economies

Caroline Kiondo, Stewart Kowalsk, Louise Yngström
DSV SecLab, Stockholm University/Royal Institute of Technology
SE-16440 Kista, Sweden
kiondo@dsv.su.se, stewart@dsv.su.se, louise@dsv.su.se

Abstract **—A most recent, phenomenon within new socio-eco-systems is the so called Virtual Economies. This paper presents an exploratory study of information security risks that are inherent with the Virtural Economies. A Dynamic Network Analysis Tools (DNAT) was used to perform a risk analysis in the Second life virtual world. The analysis indicates that the currency and user account are the most important assets. User accounts provide access to virtual trading and are critical to the flow of currency within the virtual economy. The removal of both of these from the system will affect the dynamics of the system and defeat the whole purpose of the system. The analysis further identified selling and creation of virtual goods to be important tasks in order to maintain a successful Virtual Economy. If a threat occurs that manipulates the creation of virtual goods then it would affect the trading of virtual goods between the users of the system hence affecting the economy. It is important that users who invest in such an economy to be aware of possible risks associated with this. As the field expands and more internet communities adopt this business model all parties involved need to think of strategies to protect assets that exist within this type of environment.**

Keywords - Virtual Economy; Security Risks; Dynamic Network Analysis; Second Life; Virtual Worlds

I. INTRODUCTION

A Virtual Economy is an emergent economy existing in Virtual Worlds as a result of the exchange of Virtual Goods for real or virtual currency. A Virtual World is an online environment that can be accessed by thousands or millions of users [1]. Not only can these environments be accessed by multiple users simultaneously, but the environment is persistent in the sense that it continues to exist whether or not a user is logged into the system. The Virtual infrastructure allows for inter-connectivity of users through the use of networked computers [2].

The user in this environment is represented by an avatar in the case of MMORPGS (Massively Multi-player Online Role-Playing Games) or a profile in the case of social networks. These entities have the ability to use virtual currency or real currency to obtain virtual goods and services.

Initially, the main purpose of such an economy was purely for entertainment purposes, however the demand for virtual goods and services and the value of these goods to users, has prompted users to either legally or illegally use real money to trade for virtual items. According to the European Network and Information Security Agency, as of 2008, the Real Money Trade (RMT) for virtual items was estimated at about $2 billion [3]. A variety of security risks, threats and attacks have emerged in Virtual Economies because of this. Since virtual items and currencies are only representation of code within a virtual system, there is a real world motivation to manipulate the system in order to obtain real profit.

Virtual Economies are rapidly gaining popularity not only in virtual games such as MMORPGS but also in Social Networking communities. More and more people chose to spend their free time in Virtual Worlds as compared to other forms of entertainment. KZERO an independent research firm has estimated that there are now about 1Billion Virtual World registered users [4]. Due to this popularity most real world organizations and businesses are now ceasing the opportunity to actively participate in Virtual Worlds. Amidst the widespread adoption of Virtual Worlds by various businesses and organizations, the management of risks associated in conducting businesses within such environments has yet to be studied. This paper aims to explore the various security risks inherent in this new emergent Virtual Economy.

This paper is divided into 5 sections. In the next section, we present some background to virtual worlds' economies problems and discuss some of current ongoing research in the area. In section 3, we give more detailed background on the Second life virtual world and outline some of the current security threats and security contra measures used there. In the fourth section we, present a risk analysis of Second Life using the Dynamic Network Analysis Tool. In the last section, we discuss our findings and proposal future research work.

II. VITRUAL WORLD PROBLEMS

Previous research in this area has shown that Virtual World environments are places where users are encouraged to explore new areas, create content and share the content with others. Security related problems that arise within Virtual Economies are also motivated due to the fact that "profit" can be made either within the world or on a secondary black market. Exploitation of bugs and "scamming", are becoming more and more prevalent within Virtual Economies. Obtaining real money from virtually world is a key factor in the increasing attacks experienced within Virtual Economies.

Most of the issues within Virtual Economies are those that are propagated by either sharing of accounts, or selling of advanced user accounts that is to say "power levelling". Power leveling is when one member logs in to another members account to play their character so that it can advance in the game. These kinds of problems are also based on permission settings within the systems [5]. Time and state bugs are also a problem in these types of environments because of the underlying architecture [6]. Integration of media and code from third party applications can cause bugs within the system as well. Users can also experience invasion of privacy through surveillance, unwanted marketing and revelation of on-line and off-line identities [7]. There are also issues in regards to trust when it comes to trading within a Virtual Economy. How can one make sure that they will receive a virtual item they are paying for with real money? In a study conducted in China, it was found that Chinese users conduct what is known as FCTs (Face-to-Face Transactions) where they meet in person for example at an internet cafe to perform the transaction [8]. There are users who take advantage of these trust issues present in Virtual Trading. A user purchasing a Virtual good or service can either claim that they have not received the object and ask for a refund or stop payment to their credit card account. Hence the seller incurs the loss; this can also happen in vice versa [9].

Various organized crimes do occur as a result of the value attached to virtual items within Virtual Worlds. Crimes such as fraud, gambling, hacking and robbery have been found to take place [10]. Thus in virtual worlds, where people hold valuable property, security of the virtual economies data must be a top priority. Privacy, security, and the integrity are factors that have been found to be of critical importance [11].

In regards to legal issues within Virtual Worlds, the main research conducted tries to understand how various real world laws apply within Virtual World Environments. There is quite a number of research studies that have discussed the legal implications of Virtual Property [10], [11], [12], [13], [14], [15], [16]. These papers have attempted to answer questions such as, *"What are the rights of a user in terms of virtual property?"* and how it relates to copyright laws [17],[18],[19], *What rights do users have? What jurisdiction is one under? Where the game servers and developers are located? Or where the player is located?* The general question of governance and how crime and gambling activities that are conducted within Virtual Worlds are handled in the real world [20], [21], [22], [23] are also important issues.

Other Issues that have been of particular interest to scholars are how taxes that are obtained from Virtual economic trades are handled [24], [25], [26]. Currently there is a large gray area that is undefined, and a few countries such as China and the USA have tried to pass legislation in regards to taxes. However, the governance of Virtual worlds and their implications to the society as a whole are still under study, as debates continue between governments and law officials.

A. CASE STUDY: SECOND LIFE

B. Background

To focus our research, we selected one of the dominate virtual worlds Second Life. Second Life (SL) was founded by Linden Research Inc. in San Francisco and was launched in June 2003. SL users or inhabitants are known as Residents. The residents of SL use the (L$) to trade for goods and services. As of March 2010 it was reported that there are about 826,214 users who are active and there were user transactions worth about $160 million [27].

To become a SL Resident one must register an account. In SL, there are two types of membership accounts. A basic membership, which is a free account, this type of account has certain limitations upon the user. The second type is the Premium membership which requires the user to pay a fee of US$72 per year. In return, users have additional access to technical support, the ability to own private regions, land and increased access to in world areas. Members also enjoy the benefit of receiving a weekly stipend of L$300. This type of membership is suitable for entrepreneurs, businesses and organizations wanting to develop their own islands.

C. Economy

In order to make purchases within SL for goods and services, residents need to own Linden Dollars (L$) which is the main currency within the world. A resident has several options for purchasing L$. This can be done at "Linden Web MarketPlace", the official L$ Exchange (LindeX) or other 3rd Party exchange services. Residents can buy L$ at L$ 260 for US$1 plus a service fee of US$0.30. The currency can be purchased using a PayPal account, Visa, MasterCard and other 3rd party affiliates. Apart from purchase of currency, one may choose to be employed in one of the many businesses running within SL in order to earn their L$. There is a wide range of jobs that an avatar can undertake. These include being a real estate agent, a sales person, an avatar billboard, customer service and support, being a DJ at the clubs, a dancer, answering surveys and camping to attract other avatars. Otherwise an avatar can become an entrepreneur and use their creativity to produce virtual goods such as clothes, furniture, houses and planes to sell to others in return for L$[28]**.**

Once residents possess L$ they have the ability to purchase anything from items to personalize their avatar, their homes, transportation or virtual land. The most important purchase apart from the personalization of an avatar is land ownership. Land purchased can be used to lease to other avatars, to build homes, offices, shopping malls, points of attraction, nightclubs and anything the land owner wishes to do with their land, the only limitation being creativity and skill base. The minimum amount of land purchased is about 512m².

SL has taken a different approach to its business model than the earlier traditional Virtual Worlds. In SL, the End User License Agreements (EULA) and Terms of Service (TOS) state that the residents of SL possess ultimate control over their creations giving them full rights to their intellectual property.

SL encourages its residents to create and trade their creations, unlike other Virtual Worlds. SL's main vision for its Economy is to have *"a fully integrated economy, architectured to reward risk, innovation and craftsmanship."* [29]. SL does so by granting its residents copyright to their creations. These creations, can be sold to others for Linden Dollars (L$) which can either be exchanged back to real currency hence earning an income or can alternatively be saved in a Linden Bank to accrue interest. Through virtual trade and creativity residents are able to accumulate assets.

Earlier, SL had decided to tax users for L$ earned through trading within the SL Virtual Economy. However, the residents were not very pleased with this model and felt that it restricted them from earning a substantial amount off their creations. This eventually led to a "*Second Life* Tax Revolt". SL decided to modify this model to fit its residents' needs. In this modified model the residents are only charged a flat subscription fee and for purchase of land. The value of the land, just like in the real world is determined by location, "aesthetics" and traffic [30]. Therefore the balance between the currency and trading of Virtual Goods is very important in SL's business model..

D. Some Security Threats

SL's game architecture follows the traditional structure for most Virtual Worlds, which is a massive distributed grid of client server system architecture. Specifically in SL's case they use Debian servers for their technology, where each server instance located on a server simulates each SL region. This means that several clusters of servers, host different parts of the SL world. According to SL, each item created within the environment is known as an asset within the database and is given its own Universal Unique Identifier (UUID).These assets are located on MYSQL server farms separate from the regions. During high traffic, where multiple requests occur to the databases, the servers are vulnerable to slow response times. This can cause users to experience objects loading at a slower pace than the normal rate and difficulty in accessing asset inventory, regions or searching for other users. This type of architecture is vulnerable to race conditions, where hackers can take advantage of the fact that different transactions are taking place on multiple databases hosted in different servers. The outcome of this attack is the ability for a hacker to perform *duping*, a practice that enables them to duplicate assets within the system [6].

SL's game client is open source, meaning any one has access to the code. The advantage of this approach is that SL is sharing the creative power with their users. Users can contribute modules and code that will benefit SL's current environment and its security. Furthermore, this proves advantageous to those who wish to leverage the platform for business opportunities. However, the disadvantage in this is that hackers can study the code and easily manipulate it to introduce exploits into the system [32].

Furthermore, even though corporations operating in SL have the capability of owning their own Island, the servers are remotely controlled by SL. Therefore it may be hard for them to link the system to their internal systems. They also lack control over the security implementation and consequently security measures and levels are dependent on Linden Labs and their developers.

When creating a basic membership account, currently SL does not check the identity of the user. Therefore there is a possibility for users to create multiple accounts and abuse the system. In the case of accounts that have been banned for violating the TOS, users can easily create a second account under a different name and continue to be part of the SL environment. The lack of control over the authentication of membership registration makes the environment vulnerable to people who want to perform illegal activities such as griefing, gambling and hacking. To provide security to account information, SL encrypts credentials and makes use of a secure HTTP connection.

SL users have the ability to develop client side code using the LSL scripting language. This language gives the users capabilities to enhance certain attributes of objects including animation. This is a useful feature for users to enable them to add functionality to their items. For example a user who wants to create aircrafts can use the animation functions to simulate the flying motion. When abused, this ability may give griefers and hackers the ability to cause destruction and exploit the SL environment. Furthermore, developers have the ability to create scripts that are useful and sell them to others as third party tools. The problem with this is that, if there are any bugs or vulnerabilities within the tool it proves to be a risk to the environment. There have been instances where SL management has had to restrict the use of some programs created by users due to possible malicious code and denial of service attacks.

Currently Linden Labs and its affiliate websites use cookies to keep track of user sessions. It is up to the user to enable or disable them. However, disabling cookies on the clients browser may unable some functionality when operating their systems. Linden Labs uses information stored in cookies to access client account information including transactions that take place on "The Marketplace".

SL has provided some guidelines to its users on how to deal with "Password stealers". Some scams that they caution against include users being asked to provide credentials in-world during various transactions. The only legitimate login form is when logging into SL, beyond that it is not necessary to log in again.

SL also caution against phishing scams, emails that requires users to submit their Second Life credentials and links to third party websites asking for this information. Some phishing scams may include giving free assets to users for example Linden dollars after providing passwords.

In terms of copyright management, SL does not have a legal way of protecting user creations. The only measure taken by SL is to track copied materials and manually ban users. As SL and other virtual world's grow it will be much harder to only impose such measure when protecting user assets. Furthermore, this may result in fear of using the system, as valuable assets are at stake of simply being copied by others.

SL also has a hard time enforcing real world laws within the system. The only way SL has control is by banning users who violate the TOS. If users of SL conduct crimes within the Virtual World, they are under the jurisdiction of the country where they reside in. This means that every user is governed differently when it comes to taxed income and other violations.

E. Security service and Mechansims

Within SL's environment, users' posses information that needs to be kept hidden to protect their assets. This includes information such as those within their accounts. (Log-In credentials, L$Balance and contact lists). However, information concerning assets possessed by an avatar is contained within SL Viewer Cache in an unencrypted form. Information transmitted through audio and chat can be eavesdropped by others as it is not encrypted. It is possible to observe and follow other avatars and even eavesdrop on their conversations. Furthermore, video recordings can be used to monitor and perform surveillance on other avatars within the environment without their consent or knowledge [33]. To combat issues regarding confidentiality SL does offer full control on permission settings to private region owners. Private region owners are able to choose who has access to the region and the type of information they have access to.

Integrity of the assets exchanged within SL is important to ensure that the economy is not flooded with fake or duplicate Virtual objects as this creates a loss of value. Users who sell Virtual Goods may be concerned about the possibility of their creations being illegally copied or transferred to others without their permission. This may also lead to problems concerning Intellectual Property rights. Buyers also need to make sure that they have received an authentic copy of a Virtual Good that has been purchased. It is also of outermost important that the L$ is not falsely duplicated, hence causing inflation within SL's Economy.

The availability of the SL system overall and parts of its regions are critical to the ongoing activities that promote exchange of virtual currency, trading and creation. If parts of the servers are unavailable and a user's business is located on those servers, there is a risk of loss of traffic and revenue. Instances of DOS attacks have happened within SL causing a loss of service. Activities such as griefing may also cause users to avoid certain areas hence limiting the availability of these areas.

There are users who purchase virtual goods and later contact their credit cards companies to dispute the charges. Therefore these users keep both the virtual goods and their money. These charge backs are a type of fraud propagated within Virtual Worlds that posses a business model allowing free trade of virtual goods.

Apart from the fact that users can be monitored through their behavior, avatar body language and chats, some functions within the world can be used to collect data. For example the use of the LlGet LandOwnerAt function returns data regarding a user's virtual property. Such information can be used by hackers to target user accounts. Second Life states on their privacy policy that they keep aggregated information in their databases in regards to IP addresses, session data, how SL is used in terms of frequency and specific pages visits. Also the third party affiliates have limited access to user data.

F. Stackholders

There are two models that have already derived stakeholders of Virtual Worlds at large are the Yee Motivation Model [34] and the Manninen model [35]. These two models will be used to mapped the various SL roles with different types of risks and threats. This information will prove useful in categorizing the assets for each stakeholder. SL, identifies four types of user roles, these include "Business Owners", "Creators", "Educators", "Landowners" and "Solution Providers".

In the Motivation Model created by N. Yee, [34] it is suggested that sometimes users are motivated by the structure and design of some Virtual Worlds. This model defines users' motivation according to three main factors, "Achievement", "Social" and "Immersion".

The second Model [35], has assessed stakeholders of Virtual Worlds by applying the Social Construction of Technology SCOT framework to analyze the key participants who interact with assets within a Virtual Economy. This framework divides the stakeholders into three main categories; "The Players", "Game Controllers" and "Third Parties". The first type of users, "The Players" may be divided further, in order to obtain different type of users who overlap with [34] Motivation Model. These are the "Achievers", "Socializers", "Explorers", "Competitors", "Griefers", "Leaders" and "Performers".

First and foremost because SL is a social environment, most of its players engage in making friends, chatting with others and in creation of relationships. These types of users are most likely to value their social status and the contacts they make. Therefore if they accumulate assets, those assets that give them an identity and help them form relationship with others are the most valuable to them. These users are known as the "Socializers"[35].

"Achievers" want to gain something extra from their experiences. Therefore these types of users may want to earn more money and accumulate the most virtual property. In SL, this would be the users who are entrepreneurial in nature; they are motivated the most by the feeling of achievement. These users will value their creative assets in their inventory and those that they sell to others. Also, they will value their social contacts because through these contacts they are able to sell and showcase their creations and assets. The ownership of virtual property is a very important, valuable asset to these users. From the aforementioned SL roles, "Achievers" could be "Business owners", "creators" or "landowners".

Another category of SL stakeholders are the "Game controllers"; these are the users who directly have stake in the business model of the virtual world. In SL, we can describe this category as Linden Labs the owner of SL and other third party companies who provide SL with additional infrastructure or features for their experience. In the following section the assets for these identified stakeholders is assessed as well as the various threats and vulnerabilities.

G. Assets match with vulnerablities and Threatss

After having identified the various Stakeholders of SL, their assets are analyzed and identified here. Due to space limitation only some of the assets matching to the vulnerable will be presented here

The avatar is the player's identity and the central point of existence within a Virtual World. It is through the avatar that other assets are derived and possessed. It is emphasized that an avatar as an asset is detrimental to a users Virtual World existence [35], [36], [37]. It is through the Avatar that a user possesses assets such as virtual goods and land. Since the avatar is the point of access to the SL environment, its importance security-wise is equivalent to a user account.

The account consists of login credentials including the username and passwords as the means to controlling an avatar. This account also has other important information regarding the avatar's activities within the Virtual World, including how much virtual property they own, how much virtual currency they have on their balance, business transactions and their contacts which may be friends or business clients. A hacker may try to gain access to this using social engineering, spam or malicious code, if successful they can steal the user's virtual property and continue to deceive the user's contacts as well [10].

The SL Currency Linden$ is the most valuable asset to the Virtual Economy. If a hacker is able to duplicate the currency, then the whole Economy can collapse. This can cause serious damage to all operating within SL and especially to Linden Labs. Since the currency can be exchange to real money, its loss to an individual means loss of real money and is equivalent of credit or debit card theft.

For social residents who do not trade within SL and those that have the basic account may not be affected by this asset because they may not own a significant amount of it. Residents, who are entrepreneurs, regard currency as a very critical asset, because their main reason for using SL is to earn money.

Land on SL can be used to create virtual houses where an avatar “lives”, or can be rented to others as virtual real estate or it may be an island for an organization’s business. Anshe Chung who was the first self made SL millionaire, owns land estates on multiple servers which she rents and sells as part of her main business, for an entrepreneur such as herself she cannot afford to lose her valuable land or have one of these servers hacked into. For other organizations that conduct meetings or provide distance learning, it may be important that the land is protected for unauthorized access. Loss of an Island would be detrimental in such instances..

According to the aforementioned assets, there are several threats and vulnerabilities that can pose risks to the stakeholders.

Hackers can pretend to be SL employees and easily extract important information from users. This may include information such as their user name and password. Another way a hacker can phish for this information is through a user’s e-mail. A user may receive an e-mail asking for their credentials, once they provide this information. The hacker can take control of their avatar and account information. In this case assets such as social contacts, virtual property, virtual currency and land are at risk. They can also use the avatar to con others who trust the user [38]. Phishers may also find it easy to obtain credentials in this type of environment because young people tend to have the habit of sharing their credentials. Moreover, the credentials may be used in other systems which can make it easier for hackers who phish for these credentials to gain access elsewhere as well [8]. In some cases, threats in other web applications such as emails can endanger assets in the Virtual World. In this case if a user has opened an attachment with a trojan horse which is logging activities on their computer. The hacker may gain access to the user's passwords to SL and in turn steal their virtual currency or contacts. Also the hacker may have the ability to impersonate the user and conduct social engineering attacks to friends and colleagues [39].

Organizations that have employees in SL Islands run the risk of hackers engaging in Social Engineering tactics to obtain information. A hacker can contact any employee and engage in conversations with them which may result in confidential information being given out. Hackers can then use this information to break into other systems out of the virtual world of SL. Also because most of the content in SL can be viewed by others, hackers can use this information freely to collect data for social engineering purposes which may lead to identity theft.

Cheating is a violation of EULA agreement between the user of a Virtual World and its providers. This violation employs the use of tools to ensure that tasks are automated. Cheating is usually performed via 3rd party software tools; this type of software is usually known as Bots. Cheating has been classified as a threat to the Virtual Economy, because it may include activities such as exploitation of the system to take advantage of bugs or social engineering of others within the system [40]. In the instance of SL, the use of bots can be employed to make illegal copies of other users creations. This may cause copyright infringement and loss of value to goods hence destroying other's businesses. Also, bots can be used to cause DOS attacks to the system..

Griefing is the process where other users perform activities or actions that may tarnish the image or cause damage to ones avatar, business and reputation. Griefers rely on the fact that basic accounts do not require identity verification; anybody can create an account and use it to harm damage or cause disruption to others.

Charlie Miller and Dino Dai Zovi set out to execute “a proof of concept exploit” in Second Life. In this case, the intention was to try to “steal” another user's Linden Dollars and convert it to real money.

At the time of the exploitation, Apple's QuickTime Player, which SL uses for rendering media such as audio, video and pictures contained a vulnerability. This vulnerability meant there was an opportunity to take advantage of the stack overflow. The researches created a malicious QuickTime file, hosted on their remote servers. In SL they created a cube which pointed to the URL of the malicious QuickTime file. At this point if an avatar happened to pass by the area containing the cube, a hacker could take control of the avatar. In this particular case the researchers were able to create a DLL to access functions within SecondLife including

III. Risk Analysis

The use of Network analysis tools to understand the behavior of complex systems has been employed for more than eight decades. Throughout history this science has been adopted by sociologists, anthropologists, biologists, psychologists, mathematicians and economists to study various systems that exist within the society [41]. The data collected from the Case Study Analysis of SL was formatted and analyzed in a DNAT.

To conduct analysis and extract these measurements, the Organizational Risk Analyzer (ORA) was used. “ORA is a network analysis tool that detects risks or vulnerabilities of an organization’s design structure.” It has over 100 measures with 3 classifications based on risks and vulnerabilities. It is one of the DNAT developed by CASOS in order to measure Risk in Organizations [48]. However the data input in this tool are not only limited to Organizations, one can use this tool to analyze any type of scenario that can be depicted as a network. Previous research studies which have used this tool include impact analysis of weaponized biological attacks on cities, impact analysis of actions in asymmetric warfare simulation and estimating impact of organizational downsizing.

In order to analyze data in ORA, objects are identified and their relationships are defined according to the aforementioned five elements in rows and columns. These objects and relationships form a collection of networks known as the meta-matrix. This meta-matrix is the main input that is analyzed by ORA in order to detect potential risk.

The case study analysis of SL was used as a source to extract all the information possible in order to construct the required meta-network. To accomplish this, the first step was to create nodes and nodesets necessary to build the network. The first node set created was for all the key stakeholders as identified previously. The relationship between each is mapped by a binary number ‘0’ or ‘1’. The task nodeset consisted of tasks that were needed in order to facilitate trading of virtual goods amongst the stakeholders. The knowledge nodeset was represented by those skills that were necessary to make money and socialize in the environment. The events depicted in the nodeset were those that could pose threat to the virtual economy of SL. Lastly the resource nodeset included the assets as categorized previosly. Each of the created nodes were combined to create subnetworks based on their relationships. The nodesets created for the experiment were: agent x agent, agent x knowledge, agent x resource, agent x task, agentNodeset, event x event, event x resource, eventNodeset, knowledgeNodeset, resourceNodeset, taskNodeset. All these nodesets were then imported into ORA. The outcome was a metamatrix identifying points of risk within the system. According to this input ORA performed statistical analysis to indicate probable risks within SL’s Virtual Economy.

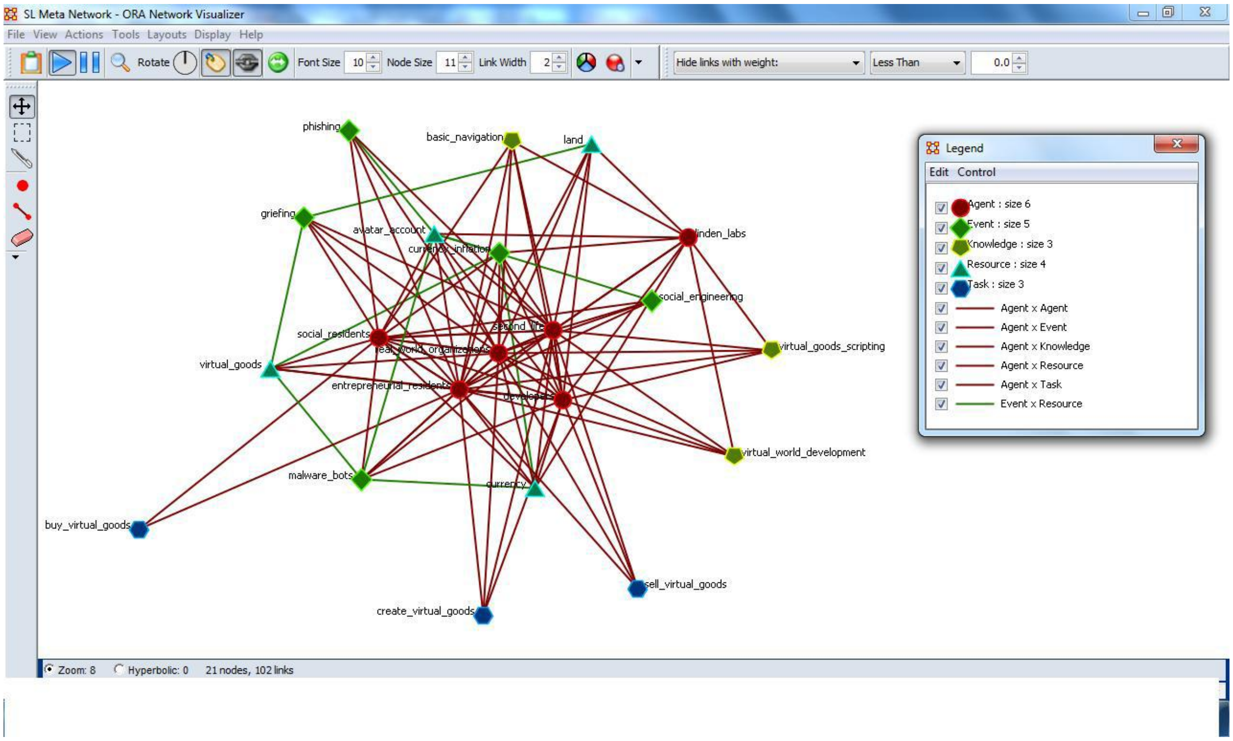
The SL Meta Network consists of six networks and five nodesets. The agent who in this case is the SL Stakeholder was the most important factor to the system. Without the stakeholders participating in SL’s Virtual Economy, the system will cease to exist. The stakeholder was analyzed in terms of the resources, tasks, knowledge, events and to each other’s interaction within the system. Finally the resources were also analyzed based on the various threats (events) that can affect them.

When visualizing the relationship between the stakeholders and the assets it is clearly demonstrated by ORA that the most critical assets are currency and avatar accounts. The currency and avatar account as critical assets relationship can be viewed by looking at the Agent X Resource Relationship within the SL Metanetwork as presented in figure 1. Also this can be seen in the relationship depicted by Agent Event X Resource. Here we can see that the currency is directly connected to the event currency inflation demonstrating its close link. Also currency appears the most central resource with the most connections, which means that removing this link from this equation will collapse the network and evidently it is a large risk. In the case of the avatar and accounts the relationship diagram shows that this is the most targeted asset. Four out five of the events are directly linked to the avatar and account asset, hence having direct impact and risk. These events are phishing, malware and bots, griefing, social engineering and currency inflation.

According to this visualization it can be concluded that the currency is the foundation of the economy and the accounts provide access to the trading of the economy. The removal of both of these from the system will affect the dynamics of the system and defeat the whole purpose of the system. All users of the system rely on these two resources to ensure that the system continues to operate at optimum efficiency. This is not to say the other resources are of no importance to the system whatsoever, it just shows that these are the most critical.

In addition to the visualization tool, various measures were used to analyze the risks of certain events within the economy. The capability measure depicted by Event X Resource shows which events are most capable of affecting each resource. This illustrated that the resources had a high risk from threats such as malware, bots and currency inflation. The malware and bots could affect the alteration of the resources and the trading of goods within the system.

Currency inflation would affect the economy by rendering the monetary value of goods useless. The Centrality measure of Agent X Resources depicted that avatar, accounts and currency as having the highest measure. This confirmed that the accounts and the currency were resources that ran the highest risk if a threat were to occur within the system. Also this measure illustrated that the creation of virtual goods and their sales were the most important tasks within the virtual economy shown by the Centrality Agent X Task.


SL Meta Network - ORA Network Visualizer

Font Size 10 Node Size 11 Link Width 2

Hide links with weight: Less Than 0.0

Zoom: 8 Hyperbolic: 0 21 nodes, 102 links

Figure 1. The Second Life MetaNetwork.

IV. DISCUSSIONS

The main goal of this paper has been to explore security risks that are inherent within Virtual Economies of Virtual World Systems. The paper outlines a high level case study analysis of the Virtual World Second Life. It is first viewed as a holistic system and the various implications to security are discussed including real world scenarios. This analysis is the basis for extraction of information regarding assets, vulnerabilities and threats within such an environment which in turn is used to construct data for risk analysis using DNA Tools.

The various stakeholders of SL's Virtual Economy were identified; also the assets that are related to these stakeholders and their threats and vulnerabilities were also identified and discussed. Finally all the data was formatted accordingly to Organizational Risk Analyzer (ORA) model which was identify Currency and Avatar/accounts being the most vulnerable assets, also that currency inflation was the biggest risk to the Virtual Economy of Second Life.

The findings have confirmed that there are real threats within Virtual Economies of Virtual Worlds, the most critical assets being user accounts and currency which are most vulnerable to malware, bots and inflation. Because of this discovery it is important for users especially those who are going to put their real resources within a Virtual Economy to be aware of the risks and how to protect themselves against these possible threats.

Future Work

According to the work performed in this paper it has become apparent that Virtual Economies are a new untapped research field. This field has a potential of becoming very important in the future as more and more social networking systems and virtual worlds embrace trading of virtual goods, especially if this new type of commerce emerges as a new platform for transaction processing on the Internet.

There are still a great numbers of questions that need to be researched in terms of security in Virtual Worlds and their economies. Specifically to complement the scenario based simulation conducted by the Dynamic Network Analysis Tool, other research methods and risk analysis techniques can be used to further explore the results and to understand their implications in a real world setting. Since the goal of this paper was to explore this new area, it hoped that other researcher can build on these findings to help individuals and organization better understand what real risks they are facing in these new virtual worlds.

REFERENCES

[1] E. Castronova, "Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier," CESifo Working Paper No. 618, December 2001.

[2] M. Bell, "Toward a Definition of Virtual Worlds," *Journal of Virtual Worlds Research*, (2008).

[3] [ENISA, "*Virtual Worlds, Real Money*," Position Paper November 2008.

[4] KZERO, "2010 Virtual Worlds and Beyond: Key Market Trends and Developments." URL:http://www.kzero.co.uk [Retrieved on May, 2011]

[5] J. Bardzel, "Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games." Situated Play Proceedings of DiGra 2007 Conference

[6] G. McGraw and G. Hoglund,"Online Games and Security," IEEE Security and Privacy, vol. 5, no. 5, pp. 76-79, Sep./Oct. 2007

[7] T. Zarsky, "Privacy and Data Collection in Virtual Worlds". STATE OF PLAY - LAW, GAMES AND VIRTUAL WORLDS, Jack M. Balkin and Beth Simone Noveck, eds., NYU Press, 2006. [8] Y. Wang, S. Mainwaring, "Human-Currency Interaction: learning from virtual currency use in China", Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, April 05-10, 2008, Florence, Italy

[8] S. Lindtner, "A Hybrid Cultural Ecology: World of Warcraft in China." In: Proc. of CSCW 2008.

[9] Y. Chen, "Online Gaming Crime and Security Issues – Cases and Countermeasures from Taiwan" Canadian Council.2004

[10] J. Fairfield,"Virtual Property" Boston University Law Review. 85, 2005.

[11] R. Reynolds, "Hands off My avatar! Issues with claims of virtual property and identity" Proceedings of Digital Games Industries(2003)

[12] I. MacInnes, "The Implications of Property Rights in Virtual Worlds." Proceedings of Tenth Americas Conference of Information Systems (AMCIS 2004).

[13] A. Eriksson and K. Gril, "Who owns my avatar? - Rights in virtual property." Proceedings of DiGRA 2005 Conference: Changing Views – Worlds in Play.

[14] [15] M. Meehan, "Virtual Property: Protecting Bits in Context." Richmond Journal of Law and Technology. (2006)

[15] A. Jankowich, "Property and Democracy in Virtual Worlds". 11 B.U.J. SCI & TECH. L. 173 2005

[16] J.M. Balkin, "Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds." Virginia Law Review. 90, 2004.

[17] P.S. Jenkins, "The Virtual World as a Company Town – Freedom of Speech in Massively Multiple Online Role Playing Games." Journal of Internet Law.8 (1)2004

[18] A.D. Schwarz and R. Bullis, "Rivalrous Consumption and the Boundaries of Copyright Law: Intellectual Property Lessons from Online Games." Intellectual Property Law Bulletin 2005.

[19] T. Burke, "Play of State: Sovereignty and Governance in MMOGs" 2004

[20] G. Lastowka and D.Hunter, "Virtual Crimes" New York Law School Law Review. 49(1) 2004

[21] I. MacInnes, Y.J Park and L S-M Whang, "Virtual World Governance: Digital Item Trade and its Consequences in Korea." Telecommunications Policy Research Conference 2004.

[22] J. Grimmelmann, "Virtual Worlds as Comparitive Law.", New York law School Law Review.47, 2004

[23] T. P Seto, "When is a Game Only a Game? The Taxation of Virtual Worlds." Loyola-LA Legal Studies 2008.

[24] B. Camp, "The Play's the Thing: A Theory of Taxing Virtual Worlds." Hastings Law Journal. 59(1) 2007

[25] L. Lederman, "Stranger than Fiction: Taxing Virtual Worlds." New York University Law Review. 82 2007

[26] M. Wagner M, 2010, "Second Life CEO looks to the future, after massive layoffs" ComputerWorld http://blogs.computerworld.com/16303/second_life_layoffs/ [Retrieved on May, 2011]

[27] M. Rymaszewski, "*Second Life: The Official Guide.*" 1st ed. Hoboken, N. J.: 2007, Wiley. ISBN 047009608X

[28] Z. Dongsong and S. Prabodh, "Doing business in Second Life: e-commerce in 3D online environment." IJEB 8(2): 148-169 (2010)

[29] C. Ondrejka, "Aviators, Moguls, Fashionistas and Barons: Economics and Ownership in Second Life"..

[30] C. Miller, "Virtual worlds, real exploits", Network Security, Volume 2008, Issue 4, April 2008, Pages 4-6

[31] C. Y. Lee, 2009, "Understanding Security Threats in Virtual Worlds". *AMCIS 2009 Proceedings.* Paper 466.

[32] N. Yee, "Motivations for play in online games". Cyberpsychol Behav. 2006; 9:772–5 2006

[33] J. Bromberger "The Social Construction of Virtual Assets: Step One: Relevant Social Groups and Interpretive Flexibility." 2006.

[34] T. Manninen and T. Kujanpהה, "The Value of Virtual Assets – The Role of Game Characters in MMOGs," *International Journal of Business Science and Applied Management*, Vol. 2, No. 1: 21-33, 2007.

[35] T. Manninen, T. Kujanp, L. Vallius, 2007, "What's My Game Character Worth – The Value Components of MMOG Characters." *Situated Play, Proceedings of DiGRA 2007 Conference*. (2007): 327-334.

[36] J. Elliott and S. Kruck, "Help – Somebody Robbed my Second Life Avatar!." Journal of Virtual Worlds Research, North America, 1, Jul. 2008.

[37] I. Muttick, "*Securing Virtual Worlds against Real Attacks",* McAfee, 2008.

[38] S. De Paoli and A. Kerr, "We Will Always Be One Step Ahead of Them", A Case Study on the Economy of Cheating in MMORPGs. Journal of Virtual Worlds Research, North America, 2, Feb. 2010.

[39] [41] H. Armstrong and I. McCulloh, "Organizational risk using network analysis." In *Proceedings of the South African information security multi-conference*, edited by Nathan Clarke, Steven Furnell and Rossouw von Solms, 132-141, Plymouth, UK: Centre for Security, Communications & Network Research, 2011.

[40] K. Carley and J. Reminga, "ORA: Organization Risk Analyzer." *Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Technical Report CMU-ISRI-04-106,* 2004