Virtual Economies: Threats and Risks

Christopher Thorpe[1], Jessica Hammer[2], Jean Camp[3], Jon Callas[4], and Mike Bond[5]

[1] Harvard University
`cat@seas.harvard.edu`
[2] Columbia University
`jh2354@columbia.edu`
[3] Indiana University
`ljcamp@indiana.edu`
[4] PGP Corporation
`jon@pgp.com`
[5] Cryptomathic Ltd
`Mike.Bond@cl.cam.ac.uk`

These notes were prepared to explore ideas developed in a panel discussion at Financial Cryptography 2007. Moderator: Jean Camp. Panelists: Mike Bond, Jon Callas, Christopher Thorpe.

1 Introduction

In virtual economies, human and computer players produce goods and services, hold assets, and trade them with other in-game entities, in the same way that people and corporations participate in "real-world" economies. As the border between virtual worlds and the real world grows more and more permeable, privacy and security in virtual worlds matter more and more.

Virtual economies first appeared as early as the late 1970's in MUDs (Multi-User Dungeons), with the advent of dial-up bulletin board systems and research computer internetworking. The earliest and simplest in-game economies simply allowed players to obtain currency dropped by slain monsters or from in-game vendors who would purchase unwanted items (usually also dropped by slain monsters). This currency could be used to buy superior weapons, armor, or training to allow the player to more effectively kill (often more powerful) monsters and thus earn more money. MUDs and related games in the 1980's began to use the in-game currencies for other purposes, such as creating in-game assets. As the complexity of MUDs grew, so did their economies, but because most MUDs were small in scope and run without profit by enthusiasts, there was little implied value in their in-game currency: the players who ran the system would simply conjure up currency whenever they or their friends needed it.

This changed substantially with commercial development of large-scale, multi-user virtual worlds designed to earn a profit. In these worlds, game designers employed scarcity to establish value; in particular, the universal scarcity of time.

Thus, virtual economies began to develop organically, with killing monsters as what might correspond to their first "natural resource" in a real-world economy. The first major success of these, EverQuest, was released in 1999, but as early as 1996, players began to exchange in-game currency and goods for real-world cash [7]. They wanted more powerful in-game characters, and were willing to spend real-world cash to effectively hire someone to do the virtual work for them. Suddenly, virtual assets had real-world value.

The past few years have seen explosive growth in participation in virtual worlds. World of Warcraft alone has over eight million subscribers worldwide [4]. Many of these "traditional" online games, including World of Warcraft, prohibit the resale of in-game assets, and Blizzard Entertainment has banned tens of thousands of accounts and removed over $1M worth of gold from its World of Warcraft economy from players who exchange gold or use third-party programs to "farm" in-game assets. Trade in these assets is fast becoming a billion-dollar industry [3].

However, some companies have recognized that the exchange of in-game assets for real-world cash is inevitable, and even profitable. Linden Labs, the creators of *Second Life*, facilitate an exchange between its currency, Linden Dollars, and US Dollars. Three Rings Design's *Puzzle Pirates* supports worlds in which players purchase "doubloons" from Three Rings, then trade them for goods and services, or in-game currency from other players, in official, market-driven in-game exchanges. MindArk's *Entropia Universe* pegs its currency, the Project Entropia Dollar (PED), at 10 PED to $1 USD.

Nonetheless, few game players actually "own" their virtual property; end-user license agreements generally make it clear that all in-game state is the property of the game developer. (*Second Life* is a notable exception in this area.) As player investment in virtual worlds continues to grow, "virtual property rights" and the security of virtual property will become important issues.

Still, most players' participation in these in-game economies is ultimately a choice, more akin to playing the stock market than to buying groceries. While players exchange their time or money for in-game goods and services, they can just as easily invest their time and money in activities of other sorts, effectively going "off the grid" in a way rarely possible in real life. Unlike participation in the economy of the real world, the choice to participate in a virtual world is entirely voluntary.

The risks and rewards of a virtual economic life often exist entirely within the "magic circle" of the game itself [11]. Even the most powerful potion of healing in a virtual world cannot heal a real-life patient! Threats to a player's in-game property or achievements are certainly serious, as these items represent an investment of time – the only truly scarce commodity and economic measure of real value in a world of infinite digital duplication. But the magic circle has leaks in it, leaks that let the risks of a virtual world penetrate the very real. Thanks to the rise of economic institutions that exchange real-world cash for the time investment necessary for play – such as eBay, Second Life's LindeX, and the official Everquest II Station Exchange – virtual assets are now very real.

Because of this real value, many security and privacy concerns have emerged that the creators of these worlds could not have anticipated. Even real-world crimes have taken place as a result of, or perhaps, as a means of perpetrating, virtual crimes. While many security threats and risks that exist in the real world do not exist in virtual economies, some of them have emerged in virtual worlds. Moreover, a new class of threats has emerged at the often blurry boundary between virtual and real economies, particulary with respect to privacy. These notes explore these classes of threats and risks.

2 Some Security Issues Don't Exist in Virtual Economies

Many important issues of security in our lives are artifacts of our real-world infrastructure. For example, because of the way money has developed, we constantly deal with security issues surrounding the possession and transfer of cash or its equivalent. In virtual economies, the creators engineer worlds in which certain problems simply can't happen — in fact, in many cases, special coding would have to be created to allow some of our nastiest problems to even exist in virtual worlds. Thus, the absence of a real-world security concern may be due either to a deliberate design choice to eliminate it, or to the simpler nature of a virtual financial existence. We illustrate this with examples.

In most virtual economies, misrepresentation of a good or service is impossible. The buyer can immediately see for herself whether the item magic spell, etc., is what it is claimed to be and reject a forgery. Fake items and goods simply can't exist unless they are specially encoded.

Players' personal assets are protected from other players in modern virtual economies. This means that a threat of in-game violence to obtain in-game benefit is meaningless. In older games, the ability of players to destroy or steal others' property or kill their characters was nearly universally accepted as a problem [8]. Solving this problem has become one of the fundamental design assumptions of today's virtual worlds.

3 Many Real-World Problems Happen Virtually, Too

The majority of real-world problems that happen in virtual worlds stem from deceptive communications. Probably the most famous is one group's infiltration of a powerful "corporation", Ubiqua Seraph, in the game *EVE Online* [2]. Over the course of a year, double agents infiltrated every level of Ubiqua Seraph, and in April 2005, murdered its CEO and took over many of its in-game assets, valued at over $16,000 USD at the time. This was completely within the rules of the game. No police investigations, lengthy trials, or prison sentences ensued; public outcries on game forums for developer redress were rebuffed. This is what distinguishes *EVE* from the real world—it's like the Wild West, and the developers want it that way.

As economies grow in complexity, so do possible exploits of them. Market manipulation is rampant; even players with modest resources can easily corner the market on certain important in-game goods, then sell the goods at a significant profit. Some players have even developed automated programs to exploit in-game markets. We know of no virtual economies that have developed anti-trust rules or price controls in their marketplaces.

Extortion occurs in various interesting new forms in virtual economies. Rather than hostage-taking or threats of violence, one *World of Warcraft* guild allegedly decided to hold in-game content hostage from the rest of the server. They were the only group on the server capable of opening a new dungeon, and posted a demand for 5,000 gold pieces from other guilds (worth approx. $300 USD at the time) before opening the gates of Ahn'Qiraj [10].

4 Virtual Economies Have Created Unique Risks

A more typical example of fraud is that a player promises to pay for a particular service, then either the buyer refuses to pay afterward, or pays first and then the seller refuses to perform the service to the buyer's satisfaction. Another example is to use a deceptive price for an item, such as charging 20 gold pieces for an item that should cost 20 silver pieces and hoping the buyer won't notice.

While this sort of fraud occurs in the real world as well, few virtual economies support written contracts or binding agreements. A player's only recourse after being defrauded is to hope the gamemasters will review server trade and chat logs and resolve the issue by "divine intervention." Some games provide such recourse; for example, in *Puzzle Pirates*, oceanmasters spend much of their time solving such problems, and because perpetrators do not benefit, such problems are rare. Conversely, in *World of Warcraft*, gamemasters generally do not have the authority to provide restitution, and the only recourse is to cry foul in public chat channels. In such games, because players who do it can get away with it, such petty thefts seem to be more common.

Bugs in the programs specifying virtual worlds create new opportunities for dishonest gamers. Sometimes, these are exploited by client players, but other times, it has been alleged that insider game developers make extra cash by selling in-game valuables. Players who discover exploits create or duplicate valuable items or in-game currency, then sell them to other players either in the game or through real-world channels to make money. Some exploits include careful timing attacks, where the player picks up a valuable item more than once or trades cash with another player, but the server doesn't properly log it. Other means have exploited bugs that take place at borders of "zones" in the game world where a player moves from one server to another. One extreme example of such an exploit resulted in a temporary 20% inflation in *EverQuest II* currency prices in August 2005 [14].

Other interesting risks that do not have real-world counterparts are still emerging. Virtual worlds at the moment seem to mimic the way people interact in real worlds, but as technology and familiarity with virtual environments improves, we may discover that there are goods and services in virtual worlds that have no real analogy in our own world, and which we do not know how to manage or regulate. This becomes especially concerning in the context of a virtual economy that "leaks" into the real world via the scarcity of time, and the consequent exchange of in-game and real-world assets. We do not yet understand the relationship of capital in establishing player-initiated goods and services; indeed, since everything is virtual once the world has been programmed, human labor — mouse and keyboard inputs — seem to be the only real input into the system.

5 The Imperfect Border: Risks Where Real-Life Meets the Virtual

In 2005, a Chinese man was stabbed to death after selling a powerful sword an acquaintance had lent him in the online game *Legends of Mir 3*. The attacker had first reported the "theft" to police, who claimed there was nothing they could do, and then took matters into his own real-life hands [1].

Gamers who do not protect their real-life identity information, including their IP address and gaming account information, have found that their in-game actions follow them home through harassing telephone calls, email, or even physical mail or personal visits.

Even when the physical world is not involved, some researchers have argued that harassment within a virtual world itself can be almost as emotionally traumatic as real-life abuse, and many claim that "virtual rape" now exists [12]. Others go further, and argue that crimes in virtual worlds are as real as crimes in our own world [5].

One can also cross the border in the other direction. For example, virtual economies can provide interesting new benefits to those of us in the real world. Brown and Thomas write that a World of Warcraft guildmaster's avocation gave him an edge in landing a senior management position at Yahoo! [6]. Some players make respectable amounts of money playing online games: Mike Everest, a high school student in Colorado, and his mother, earned over $35,000 USD in *Entropia Universe*, some of which was spent sending two siblings to college [13].

But there are risks in a permeable border between the virtual and real. Microsoft warned in a presentation at Gamesfest 2006, "Those of you who are working on massively multiplayer online games, organized crime is already looking at you." A transparent, difficult-to-trace exchange of real-world capital for virtual assets already could provide for cheap and effective international moneylaundering operations – and there is enough money flowing through these games to make such activities feasible. (MindArk, the creator of *Entropia*, reported a 2006 in-game turnover of $350M USD in trade.) Organized crime may also develop new ways of exploiting virtual economies we have yet to contemplate.

6 Conclusions

Despite these risks, virtual worlds will only increase in popularity and richness, and they contribute to our understanding of our own world in important ways. Not only do we get the chance to experiment with alternate forms of economy and governance [9], but we get to do so on a massively shortened timescale. Changes that would be impossible, or at least generations-long, in the real world, can be implemented in virtual environments in a matter of months or years. Because a developer's code allows us to constrain player actions in much the same way the laws of physics do in the real world, we can even make changes that would be impossible in reality.

While there are serious security risks in virtual worlds to both real and virtual assets, virtual worlds are also uniquely equipped to respond to these threats. Working together with game designers will be crucial here because they are not trained to consider privacy and security – they make decisions because of what is good game design. This is a good thing; security and privacy experts have important contributions to offer, and a potential role in shaping what virtual worlds might, someday, be.

References

1. ‘Game theft’ led to fatal attack. *BBC News (online)*, Mar. 31 2005.
2. Murder incorporated. *PC Gamer*, page 129, September 2005.
3. Virtual economies. *The Economist*, Jan. 20 2005.
4. Blizzard Entertainment Press Release. World of Warcraft surpasses 8 million subscribers worldwide, Jan. 11 2007.
5. S. W. Brenner. Is there such a thing as “virtual crime”? *California Criminal Law Review*, 4(1), 2001.
6. J. S. Brown and D. Thomas. You play World of Warcraft? You’re hired! *WIRED*, 14.04, April 2006.
7. E. Castronova. On Virtual Economies. *SSRN eLibrary*, 2002.
8. J. Grimmelman. *Virtual Power Politics*. New York University Press, 2006.
9. E. Harper. Cheaters slam ‘Everquest II’ economy, Feb. 20 2006.
10. J. Huizinga. *Homo Ludens*. Beacon Press, 1971.
11. R. MacKinnon. Virtual rape. *Journal of Computer-Mediated Communication*, 2(4), March 1997.
12. J. Silverstein. Are some video games gambling? *ABC News (online)*, Sept. 8 2006.
13. D. Terdiman. Cheaters slam ‘Everquest II’ economy. *CNET News.com*, Aug. 11 2005.
14. Wikipedia (English). Player killer. 2007.