Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Online Games

Jeffrey Bardzell, Markus Jakobsson, Shaowen Bardzell, Tyler Pace, Will Odom, Aaron Houssian
Indiana University
1900 E. Tenth Street #938
Bloomington, IN 47406
{jbardzel, markus, selu, tympace, wodom, ahoussia}@indiana.edu

ABSTRACT
We survey known security vulnerabilities in Massively Multiplayer Online Games (MMOGs), and describe how these are used to cheat. While such abuse often is aimed at gaining an edge in the game, there is a recent trend of financial fraud in MMOGs. We review common types of online fraud (such as phishing and click-fraud) that we believe increasingly will migrate into the MMOG sphere. We refer to the resulting abuse as *virtual fraud*. By defining a visual classification of virtual fraud, we lay a foundation to future investigations of the problem. We also use our visual classification to describe some types of virtual fraud that we believe may become particularly threatening.

Author Keywords
Click-fraud, crimeware, deceit, fraud, MMOG, phishing

INTRODUCTION
The gaming industry is seeing a rapid increase in Massively Multiplayer Online Games (MMOGs), both in terms of the number of players and in terms of revenue. What only ten years ago was an isolated phenomenon—online gaming—is now a household staple. The significance of gaming is extending its reach beyond entertainment systems, such as the Sony Playstation, as non-entertainment uses of game technologies become prevalent. Health, education, military, and marketing uses of game technologies are leading a wave of "serious games," backed by both government and private funding.

At the same time, and independently of the progress on the gaming industry, online fraud has grown at a remarkable pace over the last few years. According to the research firm Javelin, identity theft cost U.S. business $50 billion in 2004, and $57 billion in 2005—more recent numbers have not yet been publicly released, but all points to a further increase of the problem. While the costs of click-fraud in many ways are harder to estimate, among other things due to the fact that there are no post-mortem traces of it having occurred. Already in 2004, click-fraud was recognized as one of the emerging threats that online businesses face (Crawford, 2004).

An increasing number of researchers and practitioners are now starting to worry about a merger of these two patterns, in which MMOGs are exposed to online fraud or their existence facilitates an increase thereof. The former is largely due to the possibility to monetize virtual possessions, but will, with the introduction of product placements, also have a component associated with click fraud and impression fraud. The latter is due to the fact that scripts used by gamers may also host functionality that facilitates fraudulent activities beyond the worlds associated with the game. More concretely, such code may carry out phishing attacks on players, may be used to distribute spam and phishing emails, and may cause false clicks and ad impressions.

In this paper, we survey the threats MMOGs pose and may cause to pose. While our focus is fraud directly associated with any given game, we will also review indirect damages. Our goals are to introduce security specialists and game designers alike to the problems we face and to discuss particular vulnerabilities and countermeasures. To simplify the development of an understanding of existing and potential vulnerabilities and the ways in which these can be translated into fraud, we introduce a visual classification of the abuses. The classification is based on both the origins and manifestations of the problems—either could be from inside the game or from outside the game. Moreover, the classification considers the common stance to the technology from which the problem originates, and whether the use of such technology is inherently encouraged, discouraged, or neither of these. The latter is a useful aspect to consider in order to understand to what extent future trends may change the threat picture.

RELATED WORK
Comparatively little has been published on fraud in massively multiplayer online games. However, more work has been published on the related topic of cheating in games. Existing literature on both of these topics is summarized in this section.

Situated Play, Proceedings of DiGRA 2007 Conference

Fraud and Games

Chen et al. (2004) provide a useful analysis of identity theft as it pertains to crime and security in online games, with a focus on the East Asian context. In addition to a general introduction to online gaming, they explore several types of online gaming crime, especially virtual property and identity theft, relying in part on statistics collected by the National Police Administration of Taiwan. For them, identity theft is considered the most dangerous vulnerability, and they argue that static username-password authentication mechanisms are insufficient. After a review of different authentication approaches, they conclude that dynamic user authentication, with one-time password generators, is the most feasible solution for MMOGs. It should be noted, however, that the reliance on such methods does not automatically secure a system, given the risk for man-in-the-middle attacks in which the attacker obtains time-dependent credentials and then immediately starts a session with the legitimate service provider.

Cheating and Games

One growing literature of direct relevance for game security pertains to cheating in games. Cheating and fraud in games are similar but non-identical phenomena. (Yan & Randell, 2005) define cheating as follows:

> Any behavior that a player uses to gain an advantage over his peer players or achieve a target in an online game is cheating if, according to the game rules or at the discretion of the game operator (i.e., the game service provider, who is not necessarily the developer of the game), the advantage or target is one that he is not supposed to have achieved. (p.1)

Both cheating and fraud involve players misusing game environments and rule systems to achieve ends that are unfair. One primary difference between them is that whereas cheating is defined relative to the rules of the game, as defined by the game service provider, fraud involves violations of national and international law. In addition, whereas cheating is limited to the games themselves, game-related fraud may extend to external media, such as Web forums and email. Thus, the literature on cheating is useful primarily with regard to abuses in the games as more or less closed information systems; it will be less helpful with game-related fraud that exceeds the game as an information system. Game-related but external forms of attack may occur in external media, such as the aforementioned Web forums and email, or in external purpose, such as gaining access to a user's system to install malware, such as key logging software, to gain access to bank accounts that obviously are not directly connected to game play.

The most systematic overview of online cheating can be found in Yan and Randell, which offers what is intended to be a complete taxonomy of cheating in games. The authors identify three axes with which to classify all forms of cheating in games. They include the following:

- **Vulnerability**. This axis focuses on the weak point of the game system that is attacked. It includes people, such as game operators and players, as well as system design inadequacies, such as those in the game itself or in underlying systems (e.g., network latency glitches).
- **Possible failures**. This axis refers to the consequences of cheating. It includes theft of information/virtual possessions, service denial, and masquerading, among others.
- **Exploiters**. On this axis are the perpetrators of the cheating. It includes cooperative (game operator and player, or multiple player) as well as individual cheating (game operator, single player).

Though we will propose a different framework in this paper, Yan & Randell's could also be extended more generally to game-related fraud. The primary difference would be that each category would have to be extended beyond the game as an information system. Vulnerabilities, for example, would have to include technologies that enable the spreading of Trojan horses. Possible failures would extend to non-game-related forms of fraud, such as attacks that accessed banking information. Exploiters, too, would go beyond game developers and players, to any criminals that use games as part of their portfolio for attacks, without regard for whether they are themselves players or service providers.

In addition to this general work on cheating in MMOGs, work has also been done on specific forms of cheating.

Bots

A "bot" is a computer controlled automated entity that simulates a human player, potentially through the use of artificial intelligence. Bots are used to give players unfair advantages, such as automating complex processes at inhuman speeds to level characters, raise virtual money, and so on.

Golle and Duchenault (2005) propose two approaches to eliminate bots from online games, based on conceptual principles that require players to interact in specific ways. CAPTCHA tests—Completely Automated Public Turing Test to Tell Computers and Humans Apart—are cornerstones of these approaches, affording the ability to generate and assess test that the average human can pass but current computer programs can not. The second approach abandons the use of software, transforming existing game input controllers into physical CAPTCHA devices. Similar to a keyboard or joystick, the CAPTCHA device would recognize physical inputs and generate digital outputs. In essence, this system authenticates human existence by prompting players with a physical output and subsequently requiring a physical acknowledgment.

Latency

The effects of lag, or network latency, on MMOGs also affect the fairness of game play. Players with higher lag are

at a clear disadvantage to those with low lag. Lag can created by a player's geographic location (propagation delay), access technology (e.g., ADSL, cable, dial-up) and transient network conditions (congestion). Zandel, Leeder, and Armitage (2005) show that game play scenarios with high lag led to a decrease in performance, and they suggest that nefarious players can use lag to gain an unfair advantage over other players. To combat lag, Zander et al. implemented a program to normalize network latency by artificially increasing delay between players and the server for players with faster connections; as a result, game play scenarios using the lag normalization program demonstrated equal kill counts for all bots.

Player Ranking

In games, ranking systems are used to calculate accumulated player scores and serve as evaluations of players according to their game histories. Player ranking systems are necessary for the majority of MMOGs to supply players with a sense accomplishment relative to other players, and ranking systems are also important in facilitating pairings (i.e., fellow players to work with or against). Traditional ranking systems are tightly bound to the specific game client and server and do not track games hosted on local area networks. Tang et al. (2005) introduce the concept of independent player ranking systems a ranking system that is independent of specific architectures and implementations of individual games. Using a certificate-based framework and player reputation-based scoring, the system, FreeRank, reduces the potential for cheating players to hide their identity among different battle nets by creating a battle net neutral system that tracks player identity and scoring across all battle nets.

MASSIVELY MULTIPLAYER ONLINE GAMES AS A DOMAIN FOR FRAUD

Massively multiplayer online games are information systems, as are Web-based banking applications and auction sites. They are also simulated worlds, with embodied avatars, sophisticated communication and social presence tools, and participant-created content. As a result, MMOGs have both commonalties and differences compared to 2D, Web-based applications. In this section, we provide an overview of MMOGs as a domain for fraud.

Functional Overview of MMOGs

Massively multiplayer online games (MMOG) are a subset of video games uniquely categorized by a persistent, interactive, and social virtual world populated by the avatars of players. Persistence in MMOGs permits the game to run, or retain state, whether or not players are currently engaged with the game. Interactivity entails that the virtual world of an MMOG exists on a server that can be accessed remotely and simultaneously by many players (Castranova, 2001). The sociality of virtual worlds is a result of combining human players; methods for communication, such as chat or voice systems; and different mechanisms for persistent grouping.

MMOGs share the following traits with all games (Smed & Hakonen, 2003).

- Players, who are willing to participate in the game
- Rules, which define the limits of the game
- Goals, which give arise to conflicts and rivalry among the players

To these, MMOGs add network communications, economies with real-world value, and complex social interaction inside a shared narrative/simulation space. Both the rule-bound nature of games and their socio-cultural context create possibilities for fraudulent behavior, which distinguishes MMOGs from fraud at banking or auction sites. We return to these possibilities later; for now, we focus on what makes MMOGs specifically *games*, and the primary element is that it is a simulation, composed of a system of rules (Aarseth, 2004).

Rules govern the development of a game and establish the basic interactions that can take place within the game world. Two types of rules exist in computer games: game world and game play rules. Game world rules create constraints on the game's virtual world (e.g., gravity). Game play rules identify the methods by which players interact with the game (i.e., number of lives). Differences in games are primarily founded on differences in game play rules (Zagal & Mateas, 2005). Working around or manipulating these rules creates opportunities for cheating and fraud. For example, Yan & Randell describe an instance where the manipulation of a graphics card enabled players to see through what were supposed to be opaque walls, locating other players that they should not have been able to see.

One may also consider a higher level of rules, describing the hardware and software limitations associated with the devices used to play games. This is a meaningful angle to consider, given that these “meta-rules” govern what types of abuses are possible of the states of the games, e.g., by malware affecting the computers used to execute a given game, and thereby also the games themselves.

MMOGs as social spaces require further breakdown of game play rules into intra-mechanic and extra-mechanic categories (Smith, 2004). Intra-mechanic rules are the set of game play rules created by the designers of the game. The LucasFilms bug just described is an example of an intra-mechanic cheat. Extra-mechanic rules represent the norms created by players as a form of self-governance of their social space. Rules implemented by guilds, which extort new players or collude against others, would fall into this category. The interplay between intra- and extra-mechanic rules may change over time, with some game developers integrating player created extra-mechanic rules into the game to form new intra-mechanic rules.

As game worlds mature and the complexity of player interactions increase, the number and scope of the rules increases dramatically. They certainly far outstrip the complexity of the rule systems involved in online banking sites and auctions, making rule complexity one of the

distinguishing characteristics of MMOGs, from a security standpoint.

The complexity of game rules provides growing opportunity for misbehavior. Clever players may knowingly use a flaw in the game rules to obtain an unfair advantage over fellow players. Players using a game flaw for personal gain are performing an "exploit" of the game ("Exploit," 2006). Commonly, exploits are used to provide players with high-powered abilities that allow them to dominate against their peers in the competitions of the game. Given the competitiveness of gaming, and the pervasiveness of "cheat codes" built into most large-budget games and widely available on the Internet and in gaming magazines, the discovery and deployment of exploits is often tolerated and even celebrated. However, the monetization of virtual economies creates growing incentives for players to exploit the game world as a means for profit, not pleasure. The ambiguous nature of the exploit, therefore, as somewhat undesirable and yet a part of game culture, and as an act that is usually legal, creates a new conceptual and technical space for attacks. It is specifically in this area that we feel traditional cybersecurity research is lacking.

Architectural Overview of MMOGs

Network Architecture

The network architectures for MMOGs are client-server, peer-to-peer, or a combination of the models. Client-server architecture is the most common due to ease of implementation and the ability to retain complete control over game state on the server. However, the client-server model is prone to bottlenecks when large numbers of players connect to a small set of servers. A peer-to-peer architecture reduces the likelihood of bottlenecks but requires complex synchronization and consistency mechanisms to maintain a valid game state for all players (Bernardes et al, 2003). Many MMOGs, such as World of Warcraft, use the client-server model for game play and peer-to-peer for patch distribution.

Interfaces and Scripts

The client-side executable interfaces with the player using the screen and soundcard, and using input devices. Typical input devices include the keyboard, the mouse and trackballs, joysticks, and microphones. Technically, these are devices that write in unique registers associated with these devices in question, which the CPU polls after interrupts generated by the input devices are detected. This causes the contents of the registers to be transferred. Any process that can write in these registers, or otherwise inject or modify data during the transfer, can impersonate the player to the client-side executable. Alternatively, if the entire game is run in a virtual machine, the process may impersonate the player by writing data to the cells corresponding to the input device registers of the virtual machines. These processes, independently of whether interacting with a real or virtual machine, are commonly referred to as scripts.

Detecting Scripts

Techniques to detect scripts assume that all activities intrusive to the system are essentially anomalous (Sundaram, 2006). In theory, comparative cross-referencing a normal activity profile with system states can alert to abnormal variances from the established profile and reveal intrusion attempts. Statistical and predictive pattern generation are the two approaches used in anomaly detection systems. The statistical approach constantly assesses state variance and compares computational profiles to the initial activity profile. Predictive pattern generation attempts to predict future events based upon prior documented actions, using sequential patterns to detect anomalous actions.

Misuse detection schemes represent attacks in the form of a signature to detect variations streaming from the same script (Sundaram, 2006). Misuse techniques are closely tied to virus detection systems, offering effective methods against known attack patterns, while providing little prevention of unknown attacks. Pattern matching and state transition analysis are among numerous misuse detection system techniques. Pattern matching encodes known attack signatures as patterns and cross-references these patterns against audit data. State transition analysis tracks the pre- and post-action states of the system, precisely identifying the critical events that must occur for the system to be compromised.

A variety of techniques exist for detection avoidance. According to Tan, Killourhy, and Maxiom (2002), methods for avoiding detection are broken down into two broad categories. First, the behavior of normal scripts are modified to look like attacks to create false positives that degrade anomalous detection algorithms (Tan et al, 2003). Second, the behavior of attacks are modified to appear as normal scripts to generate false negatives that go unnoticed by both anomalous and signature based detection systems. An important subcategory of the latter detection avoidance method is facilitated by *rootkits* or software that allows malicious applications to operate stealthily (Kaminsky, 2006). Rootkits embed themselves into operating systems and mask an attacker's scripts from the operating system and any detection programs running within the OS.

ELECTRONIC FRAUD

Having provided an overview of MMOGs in the context of security, we now turn our attention to electronic fraud. In this section, we first provide an overview of current understandings of electronic fraud, largely as found in 2D Web applications, such as online banking and auction sites. We then propose a new framework for the study of electronic fraud, which is inclusive not only of 2D Web applications, but also of MMOGs.

Overview of Electronic Fraud

Phishing

Most phishing attacks are deception-based and involve emailing victims, where the identity of the sender is spoofed, and where the recipient typically is requested to visit a website and enter his or her credentials for a given service provider, whose appearance the website mimics. This website collects credentials on behalf of the attacker. It may connect to the impersonated service provider and establish a session between this and the victim, using the captured credentials; this is known as a man-in-the-middle attack.

A majority of phishing attempts spoof financial service providers, but the above-described techniques can be applied to gain access to any type of credentials, whether the goal is to monetize resources available to the owner of the credentials, or to obtain private information associated with the account in question. The deceit techniques used in phishing attacks can also be used to convince victims to download malware, disable security settings on their machines, and so on.

A technique increasingly common among phishers is spear-phishing or context-aware phishing (IBM, 2006; Jakobsson, 2005). Such an attack is performed in two steps: first, the attacker collects personal information relating to the intended victim, e.g., by data mining. In the second step, this information is used to personalize the information communicated to the intended victim, with the intention of appearing more legitimate than if the information had not been used.

Crimeware

Crimeware is a term generally referring to software running on a person's machine without this person's approval, or without a clear understanding of the effects of the software, some of which are harming the interests of the user of the machine. Crimeware distributors often attempt to follow the letter of the law by including circumvented descriptions of the negative effects of the software in very long and complex End User License Agreements (EULA) that users are forced to agree to in order to install the software. A recent type of crimeware, spreads in a social manner, i.e., by recommendation by friends (Stamm et al, 2007).

A common types of crimeware spies on user actions—examples of this type are keyloggers and screen scrapers. A keylogger records the keystrokes of a user, and a screen scraper captures the contents of the screen. Both of these, and can be used to steal credentials or other information, and to export associated data to a computer under full control by an attacker. Another type searches the file system of the user for files with particular names or contents, and yet another type make changes to settings, e.g., of anti-virus products running of the affected machine. Yet another type of crimeware uses the host machine to target other users or organizations, whether as a spam bot or to perform click-fraud, impression fraud, or related attacks. This general class of attacks causes the transfer of funds between two entities typically not related to the party whose machine executes the crimeware (but where the distributor of the crimeware typically is the benefactor of the transfer). The funds transfer is performed as a result of an action that mimics the actual distribution of an advertisement or product placement.

Pharming

Pharming is a type of attack, often but not always initiated by malware, that aims to "poison" the look-up tables used to translate common URLs (such as www.paypal.com) to IP addresses; the latter is the representation used by computers to determine what other network computers to communicate with. Pharming effectively causes an incorrect translation, which in turn causes connection to the wrong network computer. This is typically used to divert traffic and to capture credentials. Given that pharming can be performed simply by corruption of a user computer or its connected access point (Stamm, et al, 2006), and this, in turn, can be achieved from any executable file on a computer, we see that games and mods, which are programs that run inside of the game executable pose real threats to user security.

A Framework for Analyzing Electronic Fraud

Our ability to anticipate attack vectors is aided if we can classify and visualize them. We have developed a visualization of our classificatory system of attack vectors. This classification can be applied to bank, auction site, and MMOG fraud, though the results of each of these applications would vary significantly.

The classification considers attack vectors both inside and outside of system implementations as well as the system publisher's attitude toward the vector (Figure 1). One of our goals is to be able to account for attack vectors that are related to, but not explicitly a part of implementations (the circles in Figure 1), as well as those that occur through means that the publishers endorse, reject, and do not care about (the three layers in Figure 1). One of the problems cybersecurity experts face is that attacks may be spread across different technologies, eluding attention because stakeholders may be too parochial; for example, a game publisher is obviously responsible for the security of the game client, but ownership of security issues arising from, for example, screen scrape crimeware installed with an unauthorized game mod may be seen as external to the game publisher's responsibility. The "officially agnostic" category is also important for this reason, because attacks may combine system- and non-system-related technologies in ways that system publishers do not consider, because they are not even thinking about these other systems. For example, a bank presumably does not care about whether a user is also an MMOG player; however, an attack on a bank account that is enabled by identity theft that takes place in or because of an MMOG should be of interest to the bank.

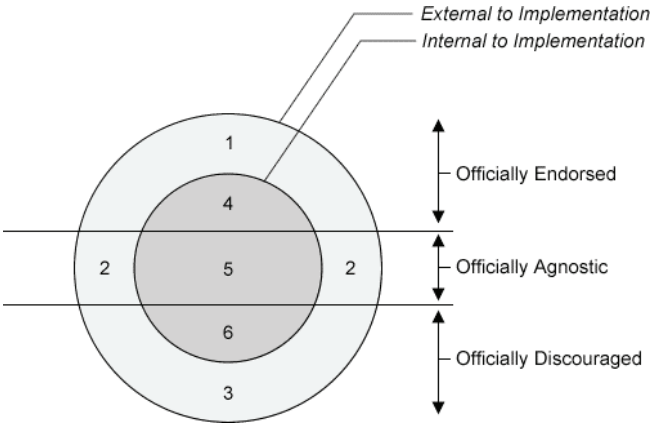

Figure 1: Potential attack vectors (numbered), distinguished by inside/outside status with regard to the system or game (the circles), and by the system publisher's endorsement, discouragement, and ambivalence (the three layers).

The figure contains two circles, representing a distinction between those features of a system that are a part of the system implementation and those that are external to it. We define a "system" as the combination of one or more back-ends and their interfaces. We define "implementation" as the set of substantial characteristics that make up a system. By "substantial," we mean those characteristics that could not be removed without changing the nature of the system, as opposed to "incidental" characteristics, which could be removed or altered without fundamentally changing the system.

For example, the fact that an online banking system uses authentication is substantial; whether that authentication system involves pins, passwords, or passphrases is incidental. The bank could change among pins, passwords, and passphrases without fundamentally altering the system, but if it removed authentication, it would be an altogether different system. Authentication is therefore internal to its implementation. In contrast, the fact that the bank sends most of its customers a bill in the mail is external to the online banking implementation, even though the same bank is responsible for mailing the bills and maintaining the online application. It is important to understand that the implementation is not necessarily limited to first-party software or features; first- and third-party characteristics may be in- or out-of the implementation. This is significant because, counterintuitively, some within-implementation attack vectors may not be the responsibility of the publisher.

The figure is also divided into three regions, from top to bottom. These regions correspond to the attitude of the institution toward a given feature. It may endorse the feature, as Citibank endorses its own Web-based banking application and its bill mailing services; it may be agnostic to it, such as Citibank's attitude toward video game use on the same machine that a user uses to connect to Citibank's Web-based services; and it may be hostile to it, such as Citibank's attitude toward phishing attacks using its name and logos. One reason we focus on official attitude is to call special attention to the agnostic category, which is both overlooked and of ambiguous accountability, two characteristics that make these vectors especially vulnerable.

Each of the numbers within the figure refers to a unique attack vector. Vector 1 refers to features that are officially endorsed and which are also external to the implementation. Number 2 refers to features that are neither endorsed nor discouraged and which are external to the implementation, and so on. Table 1 describes each of the numbers in the figure and provides examples from the online banking, auction site, and MMOG industries.

MAPPING AND OVERCOMING FRAUD IN GAMING

Our approach to mapping fraud in games is to explore each of the potential attack vectors, identify vulnerabilities, and finally explore possible countermeasures. In this section, we briefly summarize each of the six categories of attack vectors with regard to massively multiplayer online games, describing some general characteristics or weaknesses, describing some representative attack concepts for each vector, and then discussing possible countermeasures or areas for future research.

Following our classificatory framework, we divide the discussion between attack vectors external to and those internal to a game implementation.

Attack Vectors External to the Implementation

In this section we focus on attacks that occur through mechanisms that are external to the system implementation, which in this case more or less means external to the game. It therefore includes a host of issues excluded by the category of "cheating," which is relative to the games themselves. The game is a necessary, but not sufficient, condition of these attack vectors.

1. Endorsed-External

Features in this category are officially endorsed and/or they cannot be avoided without a major redesign of the system; they are also external to the implementation. Examples include official forums and Web sites, patch services, billing and account services, and so on. Because all of these are officially blessed, they are likely to be trusted. In addition, presently most of these services in the realm of MMOGs are protected by static username-password

mechanisms. Thus, features in this category are good targets for spoofing as part of phishing or pharming attacks.

For example, an attack could involve scraping meaningful information from forums to harvest email addresses, usernames, and other information that could make a phishing attack more convincing (i.e., a spear phishing attack). Alternately, an attacker could host an official patch at an unofficial location, modifying the patch with adware. Preventing attacks in this vector may involve improving authentication protocols, especially by implementing

Table 1: Explanation with examples of our classification of potential attack vectors.

#	Description	Bank Features	eBay Features	MMOG Features
1	Features that are officially endorsed or cannot be avoided without major redesign AND are external to the implementation	Monthly bill in the mail	PayPal	Billing and account services Official Web site
2	Features that are officially neither endorsed nor hated AND are external to the implementation	The user's installation and use of games on the same machine	The user installation and use of games on the same machine	Exchange of virtual and real-life currencies Unofficial forums
3	Features that are officially discouraged AND external to the implementation	Phishing Pharming Crimeware (keylogger) Absence of antivirus software	Phishing Pharming Crimeware Absence of antivirus software	Phishing Pharming Crimeware Absence of antivirus software
4	Features that are officially endorsed or cannot be avoided without major redesign AND are internal to the implementation	Online banking	Ebay.com Individual history Individual communication	Game executable Xbox Live Logout-invisibility
5	Features that are officially neither endorsed nor hated AND are internal to the implementation	Checking account and bank number can be seen on any check	Pseudonym of winner of auction is made public	Cyberdating Individual game mods
6	Features that are officially hated AND internal to the implementation	Crimeware	Crimeware	Crimeware in a patch or mod Griefing

mutual authentication.

2. Agnostic-External

Features in this category are neither endorsed nor hated, and they are external to the implementation. This vector is vulnerable in part because no one clearly owns it; that is, attacks in this vector are likely to involve technologies and to fall outside any single entity's purview. Sample features include the exchange of virtual and real-life currencies, unofficial forum and social networking sites, FAQ sites, guild sites, and other participant-created resources. Players may post sensitive data and images about themselves and others on social networking, guild, and other fan sites. Alternatively, they may engage in nefarious behavior such as deception (e.g., pyramid schemes), blackmail, bullying, and so on. The exchange of virtual for real currencies may occasion the emergence of black markets and the unmonitored exploitation they enable, including the destabilization of game currency. Sites may be created that are designed to look like fan sites (perhaps with FAQs plagiarized from legitimate fan sites) designed to draw the players to them, earn their trust, and elicit information from them.

3. Discouraged-External

Features in this category are officially discouraged or even hated, and they are external to the implementation. These include the spoofed versions of billing systems, forums, and so on. They include fraudulent email messages posing as messages from the game publisher. They also include crimeware applications that operate outside the game to steal game-related information or crimeware applications that were installed by trusting players believing they were a part of the game. Players either mistakenly trust these features or they aren't aware of their existence. As before, improved authentication protocols, including mutual authentication, should help players distinguish between legitimate and illegitimate sites.

Attack Vectors Internal to the Implementation

In the following, we continue to sketch attack vectors, focusing on those that are internal to the game implementation. Cheats tend to fall into one of these categories; however, the category is larger than the set of all cheats, because it also includes attacks that are not cheats.

4. Endorsed-Internal

Features in this category are endorsed and internal to the application. These are the most central, trusted features of them all. They include the game executable, official network sites (such as Xbox Live), the selling of virtual goods/currency for other virtual goods/currency within the same game, the ability to disappear when one logs out, in-game persistent groups (i.e., guilds or clans), and so on. One source of vulnerability is the open-source nature of some clients, such as Second Life, which exposes the code and its bugs to those who know how to find and exploit them. Players who accumulate a sufficient amount of virtual currency are potentially capable of flooding and drying up markets, single-handedly manipulating game economies in their favor. Logout invisibility also means that players can disappear at unexpected moments of transactions, disappearing with a large amount of virtual currency, never to log on again. Click fraud, which does not yet appear to be a major problem in games but likely will be, also fits in this category. Preventing these sorts of attacks can entail monitoring large, complex systems such as game economies or game rule systems, quickly detecting unusual phenomena, such as high currency fluctuation, unusually rapid character leveling, high asset turnover, high click-throughs, unexpected processing cycles or function calls in running mods, and so on.

5. Agnostic-Internal

Features in this category are those that are internal to the implementation, but about which the system publisher is indifferent. This odd-seeming category covers a number of common features, including cyberdating and other complex social activity that occurs in-world, machinima filmmaking, and any given game mods, to name a few. Put another way, these often include emergent behaviors, which occur in and depend on games as social rule systems, but which were not fully anticipated by the game designers or publishers. Yet these emergent behaviors can be deeply personal and possibly embarrassing, in the case of cybersex; likewise, they can lead to organized activities, such as gambling and casinos, whose regulation is game-world, but whose stakes are very much real-world. As such, features in this vector are particularly vulnerable to social engineering, manipulation, and extortion. In addition, as with agnostic-external attacks, attacks in this vector are not obviously the responsibility of the publisher, and so ownership of cybersecurity efforts in this area may be diffuse. Prevention of these attacks are difficult, because they are decentralized and yet internal to the main play and appeal of the game. Changes in game culture, such as education intended at raising awareness, or "street-smarts" for gamers, may be the most fruitful approach.

6. Discouraged-Internal

Features in this final category are discouraged or hated, and yet they take place inside the implementation. Perhaps the most well known of these is griefing, or virtual harassment; for example, when a high-level character kills a lower-level character over and over for no other reason than malicious pleasure. Another discouraged internal feature is the bot, which is a script that automates a player behavior. Bots in World of Warcraft, for example, run in circles and kill random monsters, automating the processes of leveling up and earning virtual gold. These two can be combined to create griefing bots, which are automated characters that harass legitimate players. Another way in is to insert malicious code into game mods, level editors, and so on. Prevention approaches include the already widespread abuse reporting mechanisms, as well as mechanisms that challenge players exhibiting suspicious behavior (such as

playing for 36 straight hours or running in perfect circles for hours) by asking questions that presumably only a human could answer.

CONCLUSION

Massively multiplayer online games produce extraordinary value for their publishers and players alike. Comprising highly complex rule systems, deployed via computer networks and systems to millions of users, they offer a surprisingly diverse array of opportunities for attacks. The security community, having focused much of its attention on 2D Web applications, such as banking systems and auction sites, lacks even conceptual frameworks for dealing with MMOG fraud. The 3D embodied simulations combined with massive social presence create new kinds of fraud that do not apply to Web applications. We also feel that existing game security research, with its emphasis on cheating, is too narrowly focused. In particular, it is comparatively weak with security vulnerabilities that are external to the game and/or about which the game publisher is ambivalent. MMOG security goes beyond the traditional responsibility of the game publisher to provide a safe executable, and this lack of clear ownership poses a challenge to the security community. We propose the concept of *virtual fraud* and a framework in which to understand it, so that we may better understand and plan to address the challenge ahead.

REFERENCES

1. Aarseth, E. 2004. Genre Trouble: Narrativism and the Art of Simulation Response. *New Media as Story, Performance, and Game*. Eds. Noah Wardrip-Fruin and Pat Harrigan. Cambridge: MIT Press.
2. Bernardes, J.L., Tori, R., Jacober, E., Nakamura, R., and Bianchi, R. 2003. "A Survey on Networking for Massively Multiplayer Online Games" *WJogos 2003*. http://www.interlab.pcs.poli.usp.br/artigos/WJogos03-Interlab-MMO.pdf
3. *BBC NEWS*. 2006. Security row upsets Second Lifers. Retrieved October 26, 2006, from http://news.bbc.co.uk/1/hi/technology/5365148.stm
4. Bourdieu, P. "Structures, habits, power. Basis for a theory of symbolic power." In *Culture/Power/ History. A Reader in Contemporary Social Theory*. ed. N. B. Dirks, G. Eley, and S. B. Ortner. (Princeton, 1994)
5. Brookey, R. and P. Booth, ``Restricted Play: Synergy and the Limits of Interactivity in The Lord of the Rings: The Return of the King Video Game." *Games and Culture* 1 (2006):214--230.
6. Caltigirone , S., Keys, M., Schlief, B., and Willshiire, M.J. "Architecture for a Massively Multiplayer Online Role Playing Game Engine." *Journal of Computing Sciences in Colleges* 18:2 (2002):105 – 116,
7. Carnegie Mellon. (2004, June 4). CERT/CC Denial of Service. Retrieved October 26, 2006, from http://www.cert.org/tech_tips/denial_of_service.html
8. Castronova, E. "Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian Frontier." 2001. *CESifo Working Paper Series No. 618*. Available at SSRN: http://ssrn.com/abstract=294828
9. Chen, B.D., and Maheswaran, M. "A Cheat Controlled Protocol for Centralized Online Multiplayer Games." 2004. *Proceedings of 3rd ACM SIGCOMM workshop on Network and system support for games*. Portland, Oregon, USA, Pages: 139 - 143
10. Chen, K., Jiang, J., Huang, P., Chu, H., Lei, C., and Chen, W. "Identifying MMORPG Bots: A Traffic Analysis Approach." 2006. *Proceedings of the 2006 ACM SIGCHI international conference on Advances in computer entertainment technology*. Hollywood, California , Article No. 4.
11. Chen, Y., Chen, P., Song, R., and Korba, L. "Online Gaming Crime and Security Issue - Cases and Countermeasures from Taiwan." 2004. *Proceedings of the 2nd Annual Conference on Privacy, Security and Trust*. Fredericton, New Brunswick, Canada. October 13-15.
12. Clickable Culture. (2006, April 16). 'Second Life' Attack Throws Avatars Sky-High. Retrieved October, 26 2006, from http://www.secretlair.com/index.php?/clickableculture/entry/second_life_attack_throws_avatars_sky_high/
13. Dickey, C., Zappala, D., Lo, V., and Marr, J. "Low Latency and Cheat-proof Event Ordering for Peer-to-Peer Games." 2004. *Proceedings of the 14th international workshop on Network and operating systems support for digital audio and video*, Cork, Ireland, Pages: 134 – 139.
14. "Exploit." From Half-Real: A Dictionary of Video Game Theory. http://www.half-real.net/dictionary/#exploit. (Accessed October 26, 2006)
15. Golle, P. and Duchenault, N. "Preventing bots from playing online games ." *Computers in Entertainment* 3 :3 (2005):3
16. Information Week. (2006, May 2). Trojan Snags World of Warcraft Passwords to Cash Out Accounts. Retrieved October 26, 2006, from http://www.informationweek.com/news/showArticle.jhtml?articleID=187002835
17. Kabus, P., Terpstra, W., Cilia, M., and Buchmann, A. "Addressing cheating in distributed MMOGs." *Proceedings of 4th ACM SIGCOMM workshop on*

Network and system support for games. Hawthorne, NY , Pages: 1 - 6 , 2005

18. Kaminsky, D. "Explorations in namespace: white-hat hacking across the domain name system." *Communications of the ACM* 49:6 (2006):62-69.
19. Li, K., Ding, S., McCreary, D., and Webb, S. "Analysis of State Exposure Control to Prevent Cheating in Online Games." *Proceedings of the 14th international workshop on Network and operating systems support for digital audio and video*, Cork, Ireland, Pages: 140 – 145, 2004
20. Malaby, T. "Parlaying Value: Capital in and Beyond Virtual Worlds." *Games and Culture* 1 (2006):141 - 162.
21. Netcraft. (2005, April 19). DDos Attacks Target Final Fantasy XI. Retrieved October 26, 2006, from http://news.netcraft.com/archives/2005/04/19/ddos_attacks_target_final_fantasy_xi.html
22. Netcraft. (2005, September 28). Scams Targeting Online Games: Old Phish With Fresh Bait. Retrieved October 26, 2006, from http://news.netcraft.com/archives/2005/09/28/scams_targeting_online_games_old_phish_with_fresh_bait.html
23. NewsGuide.us. (2006, August 8). Microsoft: MMO games face security risk. Retrieved October 26, 2006, from http://www.newsguide.us/technology/Microsoft-MMO-games-face-security-risk/
24. Security Focus. (2005, November 3). World of Warcraft Hackers using Sony BMG rootkit. Retrieved October 26, 2006, from http://www.securityfocus.com/brief/34
25. Smed, J. and Hakonen, H., "Towards a Definition of a Computer Game." *Technical Report 553*, Turku Centre for Computer Science, 2003. http://staff.cs.utu.fi/~jounsmed/papers/TR553.pdf.
26. Smith, J. "Playing dirty, understanding conflicts in multiplayer games." *5th annual conference of The Association of Internet Researchers*. 2004. http://jonassmith.dk/weblog/uploads/playing_dirty.pdf
27. S. Stamm, Z. Ramzan, M. Jakobsson, "Drive-By Pharming," Technical Report TR641, Indiana University, December, 2006
28. Sundaram, A. "An Introduction to Intrusion detection." *Crossroads* 2: 4 (1996)
29. Tan, K. Killourhy, K., Maxion, R. "Undermining an Anomaly-Based Intrusion Detection System Using Common Exploits." 2002. *Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection*.
30. Tang, L., Li, J., Zhou, J., Zhou, Z., Wang, H., and Li, K. "FreeRank: Implementing Independent Ranking Service for Multiplayer Online Games ." *NetGames'05*, October 10–11, 2005, Hawthorne, New York, USA.
31. Terra Nova. (2005, September 8). Virtual World Phishing. Retrieved October 26, 2006, from http://terranova.blogs.com/terra_nova/2005/09/virtual_world_p.html
32. Tom's Hardware. (2006, May 4). Trojan horse steals passwords from World of Warcraft players. Retrieved October 26, 2006, from http://www.tomshardware.co.uk/2006/05/05/trojan_steals_wow_passwords/
33. Yan, J. and Randell, B. "A Systematic Classification of Cheating in Online Games." *NetGames'05*, October 10–11, 2005, Hawthorne, New York, USA.
34. Zagal, J., Mateas, M., Fernandez-Vara, C., Hochhalter, B. and Lichti, N. (2005) "Towards an Ontological Language for Game Analysis." *Proceedings of the Digital Interactive Games Research Association Conference*, Vancouver B.C., June, 2005. http://www.cc.gatech.edu/grads/z/Jose.Zagal/Papers/OntologyDIGRA2005.pdf
35. Zander , S., Leeder, I., and Armitage, G. "Achieving Fairness in Multiplayer Network Games through Automated Latency Balancing." *Proceedings of the 2005 ACM SIGCHI International Conference on Advances in Computer Entertainment Technology*, Valencia, Spain, Pages: 117 - 124 2005