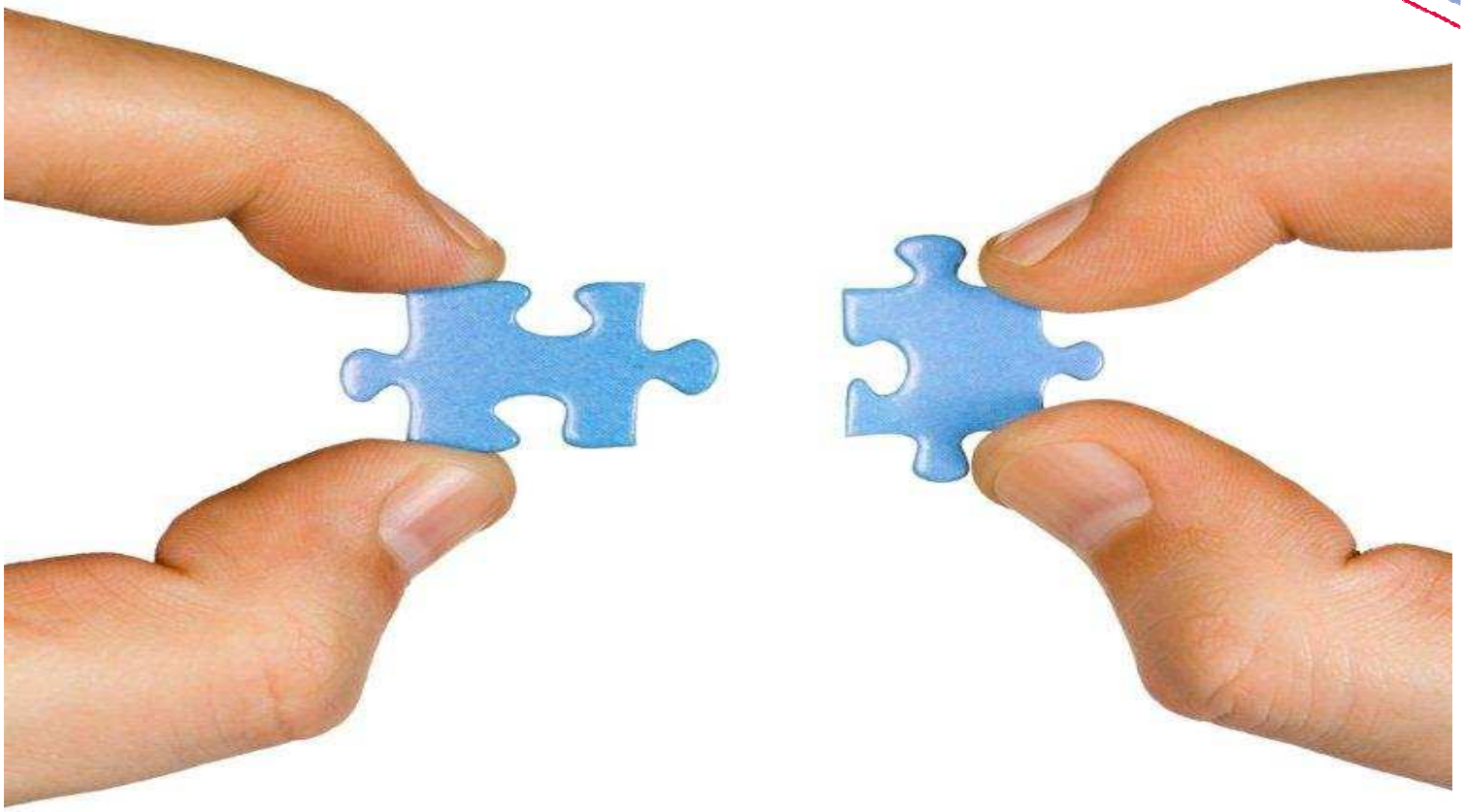
Position Paper

November 08

Virtual Worlds, Real Money

Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds



enisa
European Network and Information Security Agency

www.enisa.europa.eu

About ENISA

The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of expertise for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard of information for good practices. Moreover, the agency facilitates contacts between the European institutions, the Member States and private business and industry actors.

List of Contributors:

Experts participated as individuals. This paper should therefore not be taken as representing the views of any company or other organisation, and does not in any way bind group members when dealing with the issues it covers in other contexts.

- David Barroso, S21sec, Spain
- Richard Bartle, University of Essex, UK
- Patrice Chazerand, PEGI Online, France
- Melissa de Zwart, Law Faculty, Monash University, Australia
- Jeroen Doumen, University of Twente, Netherlands
- Slawomir Gorniak, ENISA, Greece
- Eyjólfur Guðmundsson, CCP Games
- Mateusz Kaźmierczak, UPC, Poland
- Markku Kaskenmaa, Sulake Corporation, Finland
- Daniel Benavente López, ISDEFE, Spain
- Adam Martin, NCSoft, UK
- Ingo Naumann, ENISA, Greece
- Ren Reynolds, Virtual Policy Network, UK
- Janice Richardson, Schoolnet, Belgium
- Christian Rossow, Institute for Internet-Security, Germany
- Anna Rywczyńska, CERT Polska, Poland
- Michael Thumann, ERNW IT Security, Germany

Editor:
Giles Hogben,
ENISA (European Network and Information Security Agency)

Examples are given from a number of providers throughout the paper. These should be taken as examples only and there is no intention to single out a specific provider for criticism or praise. The examples provided are not necessarily those most representative or important, nor is the aim of this paper to conduct any kind of market survey, as there might be other providers which are not mentioned here and nonetheless are equally or more representative of the market.

Contact details:

For general enquiries about this Position Paper, please use the following details:
Email: positionpapers@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

Terminology and Abbreviations

Avatar	Graphical representation of a character used in MMO/VWs
CC	Credit card OR Creative Commons
Chargeback	Reversal of a credit card payment after a transaction.
DDoS	Distributed Denial of Service
EULA	End-user License Agreement
Ganking	Attacking another player without warning, attacking while the targeted player is already engaged in combat with a non-player character, usually meaning they're distracted and/or their health has been compromised, or attacking where the targeted player is at a high level disadvantage
Griefing	Playing a game simply to aggravate and harass other players
Guild	A group of players who regularly play together in a MMO/VW
IP	Intellectual Property
MMORPG	Massively Multiplayer Online Role Playing Game
MMOG	Massively Multiplayer Online Game
MMO	(Shortened version of) Massively Multiplayer Online Role Playing Game
NPC	Non-player-characters – automated avatars controlled by the service provider
ODR	Online dispute resolution
RL	Real Life
RMT	Real Money Trade
SP	Service Provider
Shard	A subdivision of an MMO/VW, usually served by a single server.
ToU	Terms of Use
ToS	Terms of Service (equivalent to ToU)
VW	Virtual World

Executive Summary

2007 was the year of online gaming fraud – with malicious programs that specifically target online games and virtual worlds increasing by 145% and the emergence of over 30,000 new programs aimed at stealing online game passwords. Such malware is invariably aimed at the theft of virtual property accumulated in a user's account and its sale for *real money*. With nearly 1 billion registered users of MMO/VWs (Massively Multiplayer Online Games and Virtual Worlds) and real-money sales of virtual objects estimated at nearly US$ 2 billion worldwide at the end of 2007, this is a serious issue. The failure to recognise the importance of protecting the real-money value locked up in this grey-zone of the economy is leading to an exponential increase in attacks targeting online MMO/VWs.

Another important area of risk is the disclosure of private data. MMO/VWs are commonly perceived as being completely separate from the real lives of their users and therefore immune to privacy risks. In reality, representing yourself as an avatar is little different from using any other form of online persona. The inclusion of IRC and VOIP channels, along with the false sense of security created by MMO/VWs, leads to significantly increased disclosures of private data such as location and personal characteristics.

The main body of this report describes in detail these risks and others, including in-game access-control vulnerabilities, scripting vulnerabilities, denial of service, spam and threats to minors, before making a number of recommendations on how to remedy them.

Risks

1. **Avatar identity theft and identity fraud:** theft of account credentials (username and password). The main motivation is real-money financial gain, but identity fraud can also be used to damage reputation (real-life or, more commonly, in-world) and to avoid responsibility for crime.

2. **MMO/VW privacy risks:** In privacy terms, avatars are no different from other forms of online persona. Users may even disclose *more* personal data because the MMO/VW gives a false sense of security. There is also a trend towards behavioural marketing by "eavesdropping" on avatars.

3. **Automation attacks:** Some forms of automation are very problematic for service providers because they allow attackers to obtain objects or services "for free". This leads to loss of in-game value for other users, disruption of game-play and loss of revenue for service providers.

4. **Cheating, security issues:** Cheating can be a serious problem both for users and service providers. We look at categories of cheating from an information security point of view, eg, illegal object duplication (duping) and insider trading.

5. **Harassment:** In-game harassment, such as ganking and verbal harassment, can be just as serious a threat to real-world people and resources as any other kind of online harassment.

6. **Trading and financial attacks – credit card chargebacks:** Whenever an in-game purchase is made with an online payment service (eg, credit card or Paypal), a full refund can be claimed from the payment company (usually within a month). Retailers then lose money - *even if* the consumer has already made full use of the service paid for. For instance, in Second Life, it is possible to spend tens of thousands of dollars on a single purchase of land, and then split it into a large number of sub-plots, which are sold on**.** If a chargeback is issued, reversing these transactions is technically and administratively very problematic.

7. **Risks to intellectual property:** Original works can be created in-world using official tools provided by the service provider. Original work can even be created by arranging virtual objects, eg, sculptures from virtual coke cans. The actual rights held by the user are often only vaguely defined and may be invalidated by underlying rights. Also, users of virtual worlds often import copyrighted material without the permission of the copyright owner.

8. **Information security related risks for minors:** Minors can be exposed to inappropriate content in MMO/VWs either through the circumvention of age-verification techniques or the failure of content rating systems. This exposes them to risks such as disclosure of real-world contact data and pornographic or violent images.

    a. **Failure of age-verification techniques:** No currently available technique performs satisfactorily in MMO/VWs. We look at problems with existing methods.

    b. **Weaknesses in content-rating schemes:** Effective age-based content-rating systems are particularly challenging when applied to MMO/VWs because some content is determined by the end-users and the (dynamic) game culture.

9. **Problems with online dispute resolution (ODR) in MMO/VWs:** Effective ODR is particularly problematic in MMO/VWs because many disputes are raised in order to gain advantage over other players or residents. In 2006, Second Life received one ODR request per day for every 15 users.

10. **MMO/VW spam:** many bots (scripted avatars) exist within MMO/VWs, which peddle unsolicited marketing as well as offers and/or advertising services or products banned by the service provider.

11. **MMO/VW specific denial of service (DoS) attacks:** Scripted objects and avatar action in MMO/VWs provide novel variants of DoS attacks. MMO/VWs are especially vulnerable to DoS attacks because of their centralized architecture and poorly authenticated clients.

12. **Malicious game servers:** Malicious game server software can be used to perform "virtual mugging" – theft of account details or objects of value. This risk is especially important in the emerging open MMO/VW architectures where MMO/VWs may be hosted on unauthenticated servers.

13. **Attacks on user's machine through game client:** A game client is a piece of network software with specific vulnerabilities that may allow an attacker to control a user's machine.

14. **Access and authorization problems in MMO/VWs:** Attacks on access control restrictions to parts of the MMO/VW world can allow attackers to access private sectors or data. On the other hand, avatars may collude to "physically" block other avatars from a sector of MMO/VW space.

Vulnerabilities in corporate worlds: Apart from the obvious vulnerability of sensitive corporate data, it is difficult to apply and enforce a corporate IT policy in such environments.

Recommendations

To the European Commission and National Governments (Government Policy Recommendations)

1. Support the setting up of an industry-wide forum for MMO/VW service providers to share information and best-practice on security vulnerabilities. In such a competitive sector there is a clear need for a neutral forum to exchange information on security incidents for the benefit of all concerned. Given its mandate to foster a culture of information security and bring together stakeholders in Europe, ENISA would be in a good position to stimulate such an initiative.

2. Fund work on legal clarification of key issues, such as the status of intellectual property, acceptable risk and personal information in MMO/VWs. Although this is not an information security issue per se, a lack of legal clarity is at the root of many information security problems identified in this report and therefore an effort to address this issue by appropriate bodies should be part of the solution. NB: This is not a call for extra legislation but only a call for clarification and interpretation of existing legislation.

3. Encourage and fund independent dispute resolution for player-to-player disputes.

4. Create financial procedures appropriate to MMO/VWs in order to prevent virtual asset theft using chargebacks. Again, this is not an information security issue per se, but it is a root cause of the information security problems identified in this report. This should be in partnership with MMO/VW providers, banks, credit companies and online payment services.
5. Investigate and address MMO/VW provider concerns about conflicting obligations brought about by legislation on common-carrier status.

To MMO/VW providers

6. The five most important technical issues to be highlighted in this area (see full report for more details) include item-duping, end-to-end security and MMO/VW specific denial of service. In general, providers should create an appropriate balance between security measures aimed at detection and response and those aimed at prevention. Detection and response is often a more effective means of addressing security issues in MMO/VWs than prevention.

7. Privacy policies should clearly specify data collected as part of anti-cheating measures and data available to other users (eg, via eavesdropping), including any information which might identify a user uniquely.

8. Providers should consider charging a token, returnable lodgement fee for all ODR complaints to prevent false complaints (eg, €50).

9. Any initiative which increases the strength of user authentication (while maintaining an appropriate balance between usability and cost) should be encouraged.

10. We recommend a standard set of governing documents and terminology, a single point of reference where governing documents may be obtained, and the input and participation of end-user groups in their design and development.

11. As an option for more security-conscious users, in certain MMO/VWs, a bootable CD image (Live CD) containing necessary software can be made available; this is already a well-known measure to improve security in critical online operations such as online banking.

Awareness raising and research

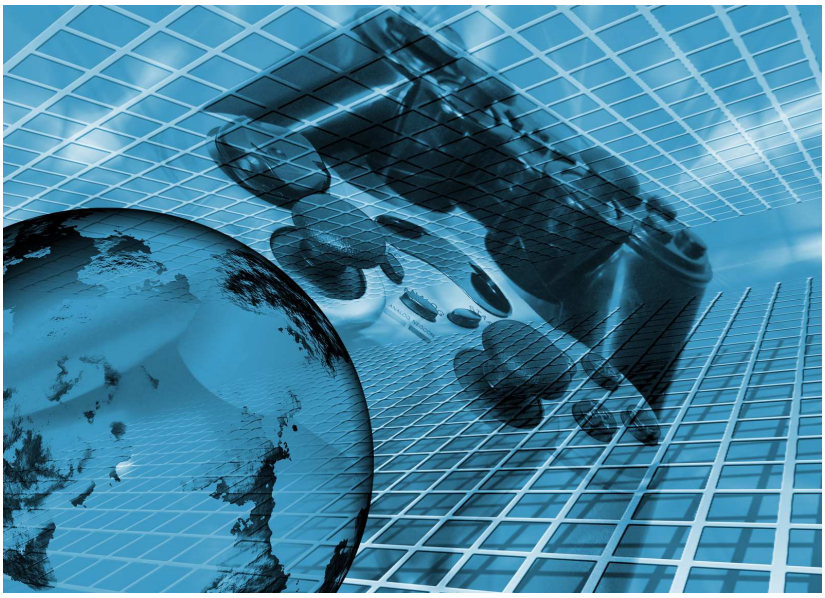
12. Awareness raising: We describe issues to be highlighted in awareness raising campaigns, such as how to detect account theft, how to deal with inappropriate behaviour, privacy risks, in-world property risks, etc.

Research: The group has identified some future trends emerging in MMO/VWs which have important security implications, including effective content filtering for MMO/VWs, security and reliability issues of open world formats, and security vulnerabilities in corporate worlds.

Security And Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds

Consensus Process

This paper was produced using contributions from a group selected for their expertise in the area. The group includes industry, academic, government and legal experts. The content was collected via wiki, mailing list and telephone conferences, and edited by ENISA. The final version was reviewed and agreed by the people listed above.



Why should you read this?

ENISA position papers represent independent expert opinion on topics ENISA considers to be important emerging risks. This paper provides an overview of the key risks to users of Massively Multiplayer Online Role-Playing Games and Virtual Worlds (MMO/VWs) and makes recommendations for actions and best-practices to address them. It is also aimed at raising awareness among political and corporate decision-makers of the legal and social implications of security issues in MMO/VWs.

Scope

We define the virtual and game worlds covered by this paper according to these criteria:

- They are shared and persistent – all participants of the world see the same world (even if from different perspectives) – and the data defining this world is usually stored in a central database controlled by the service provider.
- Interactions occur in real-time.
- There is an underlying automated rule set, the 'physics' that determines how individuals effect changes.
- Individuals are represented within the world as 'avatars' (1).

We look at four broad classes of worlds (based on Reynolds (2)) and the security-relevant features of each type:

- Civic Worlds, eg, Second Life
- Game Worlds, eg, World of Warcraft, Entropia Universe
- Social Worlds, eg, There, Habbo
- Corporate Worlds, eg, Qwaq, Forterra (See 5 Appendix I Classes of MMO/VWs). The use of virtual environments of this kind within corporate settings is a growth area and one which carries some unique risks.

Note that we do not include online gambling, because the risks are quite different. For brevity, we refer to games and worlds within the scope of this paper as MMO/VWs throughout.

The objective of this paper is to highlight and address the privacy and security risks in MMO/VWs. Such emphasis does not deny, discount or diminish the social, educational and economic value of virtual worlds. In fact, by highlighting possible risks and providing recommendations on how to minimise them, this paper offers strategies to improve privacy and security without compromising the benefits of MMO/VWs.

End-user Survey

In conjunction with this study, we conducted a survey of 1,500 end-users of MMO/VWs which may be found Gaming and Virtual Worlds Survey Results (3). We have cited parts of the result set throughout this paper where this supports our statements. We recommend, however, that the reader review the full results of the survey as an important addition to the findings presented here.

1 Introduction

Kaspersky Labs named 2007 as the year of online-world fraud. The figures speak for themselves. The number of malicious programs specifically targeting online games increased by 145% in 2007, with over 30,000 new malicious programs aimed at stealing online game passwords (4). Such malware is invariably aimed at the theft of virtual property accumulated in the user's account. The crucial factor motivating this form of cybercrime is that virtual items can be sold for real-world money, either legitimately or on the black-market. Although amounts stolen from each individual may be smaller compared to Trojans that steal credit card numbers (at least for now – see (5)), prosecutions are low or non-existent and volume is high. Virtual worlds are a soft target for thieves because they fall outside many of the measures taken to protect other online assets. With nearly 1 billion registered users of online games worldwide and real-money sales of virtual objects estimated at nearly US$ 2 billion at the end of 2007 this is a serious issue[1] (6).

A common attitude to virtual world and gaming assets is that they are "just a number in a database" or "monopoly money" and because the identity or property is not tangible and "just a game", such threats are trivial. This approach overlooks a number of very serious emerging risks. Even Euros and US Dollars are usually "just a number in a database somewhere" and are commonly used in exchange for objects or services which might seem trivial to some. Euros and other tangible or intangible assets are however protected by a long tradition of regulation which surrounds traditional economies, while assets in virtual world economies are not. This is one of the major factors leading to the growth in malware targeted at online games and virtual worlds because criminals can act with impunity.

Strange though it may seem, virtual property has considerable real money value within the global economy. For example, the Swedish company Mindark claimed a real money turnover in 2006 for trading within the world Project Entropia of US$ 360 million (7) – (see also the Mindark Annual Report (8)) and sold a virtual bank license in May 2007 for a record-breaking sum of US$ 99,900.

[1] Estimate of global MMO/VW user base using various sources eg, Habbo hotel officially has over 100 million. Kart Rider officially has 140 million (according to stock market filings for Nexon). Many Chinese games have officially reported figures of 20-80million each – as reported in Stock Market filings.

As a further illustration of the value attached to virtual property, Project Entropia and World of Warcraft (9), two of the most popular online games with over 10 million regular users worldwide (10), now offer two factor authentication solutions for authentication (11) (12). The Finnish gaming company, Sulake Corporation, was recently valued at US$ 1.25 billion and in September 2008, its main product, Habbo, had 108 million users (13) (14). Despite attempts by some game-creators to isolate virtual worlds from real-world economies by banning out-of-world transactions, there is an increasing cross-over between the two. Services already offer trading and data for currency exchange between virtual and real-world currencies (15) and virtual goods are sold on real-world auction sites such as eBay (16). Although many MMO/VWs discourage out-of-world transactions, some, such as Second Life and Project Entropia, explicitly encourage such a cross-over by publishing official exchange rates between real and in-world currencies.

Always quick to "follow the money", criminals are increasingly exploiting cross-over points between virtual and real-world economies. It is the failure to recognise the importance of protecting the real-world value locked up in this grey-zone of the economy which is leading to the "year of online world fraud". Criminal exploitation falls into three main categories:

- Theft of identity credentials (abuse of authentication).

- Exploitation of flaws in the in-world economy. This includes so-called "duping" (illegal duplication of objects), and other forms of cheating such as illegal automation and "gold farming", the virtual equivalent of sweat-shops where low paid workers work long hours to produce valuable assets within worlds (17). All practices of this kind usually result in inflation of in-game currency and loss of value to bona-fide players.

- In-game theft – the exploitation of a game feature to defraud another player of an asset. For example, in 2007, a flaw in the implementation of Quicktime within the world Second Life allowed hackers to carry out virtual pick-pocket attacks on other world residents.

Another important area of risk is the disclosure of private data. Virtual worlds are commonly perceived as being completely separate from the real lives of their users and therefore immune to the privacy risks posed by other emerging platforms such as social networks. In fact, representing yourself as an avatar is little different from any other form of online persona – users are free to present as accurate or inaccurate a picture as they choose. Some virtual worlds, such as Kaneva and Habbo Hotel may even be seen as 3-dimensional versions of social networks and users tend to give away significant sensitive personal information through channels such as chat or voice. It may even be that, because avatars and the fantasy environment give an illusion of anonymity to interactions, users tend to give away even more sensitive personal data in the more fantasy-based MMO/VWs. This is supported by the results of ENISA's survey which showed that 39% of users thought that avatars do not present any risk to personal data (18).

Even where information is not explicitly revealed, certain characteristics of the avatar owner can be guessed with reasonable accuracy based on statistical analysis and data mining. This is the case even in game worlds, where the tendency is more towards fantasy personalities. For example, a 2001 survey of the fantasy game Everquest showed that only 2.5% of female users and 15.7% of male users had played characters of the opposite gender – ie, if an avatar in this game is male, his owner is 97.5% likely to be male (19). The inclusion of IRC and VOIP channels in MMO/VW leads to significantly increased disclosures of private data such as location and personal characteristics disclosed through voice and use of language.

The use of virtual worlds as social and business platforms (among other factors) is leading to pressure on virtual world providers to provide open-source services and exchange formats. Several open architectures are already emerging in the area (20). For example in July 2008, Google issued a first version of Lively, a plug-in platform for including 3D virtual environments within web pages. IBM and Linden Labs recently demonstrated an "avatar teleporting" from the Second Life Preview Grid into a virtual world running on an OpenSimulator server (21) (22). This development parallels evolution between the Internet as a networked set of silo applications to the web as an open platform. Some sources are in fact predicting the evolution of a 3D web where, instead of linking, users would "teleport" avatars between linked areas of virtual space (23) (24). This trend introduces another set of vulnerabilities since the identity and trustworthiness of the provider and hosting servers are more difficult to establish. It enables new variants of phishing and "virtual mugging" where avatars are lured into malicious areas of virtual reality. In such an environment, the control of virtual assets is a much more difficult problem to solve.

The main body of this report describes in detail these risks and others, including in-game access-control vulnerabilities, scripting vulnerabilities, denial of service, spam and threats to minors, before making a number of recommendations on how to remedy them. The objective of this paper is to highlight and address privacy and security risks in virtual worlds and gaming environments. Such emphasis does not deny, discount or diminish the social, educational and economic value of virtual worlds. In fact, by highlighting possible risks and providing recommendations on how to minimise them, this paper offers strategies to improve privacy and security without compromising the benefits of virtual worlds.

2 Security-Relevant Features of MMO/VWs

MMO/VWs are self-contained worlds and therefore have an almost infinite variety of possible scenarios. So instead of trying to extract vulnerabilities from scenarios, we identify a set of security-relevant features in order to focus on likely areas of vulnerability. These features are present in some form in all four classes of MMO/VWs and the way in which they are implemented defines the vulnerabilities to which the world is exposed. Appendix I shows a comparison between the implementation of each security-relevant feature for a typical example of each class of MMO/VW.

We now describe each of the security-relevant features before going on to list vulnerabilities. For ease of reference, we list the related vulnerabilities and threats for each security-relevant feature.

2.1 Trading possibilities

An important source of vulnerabilities is the trading of virtual objects and services. The ENISA survey showed a very high proportion of users (56% at least monthly) doing some kind of business within an MMO/VW (18). It is important to note that, in most MMO/VWs, the contract with the player is such that they have NO legal title to anything being exchanged. The following describes the possible trading scenarios in MMO/VWs.

2.1.1 Trade with companies

There are enterprises that specialise in virtual world business, eg, IGE MMORPG Services (25). Their business is to obtain and sell goods and services (using employees working in the MMO/VW 24 hours a day):

- Virtual property (items).
- Virtual currency.
- Accounts.
- Services – eg, tips, tricks and guides on how to reach required objectives.
- Power levelling - granting access to your account to someone who plays for you until the required objective is reached.

These virtual goods are sold to the players for a value which depends on the difficulty of obtaining them. Payment can be made by credit card or by many other online methods, such as Paypal, Western Union, and Moneybookers or even via cell phone. The communication between enterprise and customer is via Internet, usually by email, and even chat. Instant messenger systems are very often used. This type of business is

governed by reputation and feedback scores on the quality of the goods or services delivered.

2.1.2 Trade between individuals

Some MMO/VW related trades happen between private individuals outside the world without any form of control. One of the most popular sites to find such trading opportunities is eBay. Again, some payments are made via credit card but most of them are made by bank transfer or by online payment companies such as Paypal. Here, the reputation of the seller is an important factor.

Trading contacts are often made within the game with actual trades being executed outside the game. This happens despite such trades being forbidden according to the MMO/VW EULA. Guarantees from the seller are rare and almost impossible to enforce. In this type of relationship, the seller's reputation is not a factor, making it a common way to scam people and get their personal information.

2.1.3 Typical trading scenarios

2.1.3.1 Trade window

- Party A: Opens trade window
- Party A: Places virtual object X into trade window
- Party B: Sees object in trade window
- Party B: Places virtual object Y into trade window, where Y might be:
  - a virtual artefact
  - an amount of virtual currency
- Party A: OKs exchange
- Party B: OKs exchange
- Items are exchanged simultaneously

2.1.3.2 Dropping

- Party A: Selects item in inventory
- Party A; Drops item
- Party B: Selects item
- Party B: Puts item in inventory
- Money is exchanged through another channel (eg, through Paypal)

2.1.3.3 Direct Transfer

- Party A: Selects item in inventory
- Party A: Selects party B
  - their avatar
  - their profile
- Party A: Transfers object to party B

- Party B: Accepts object
- Money is exchanged through another channel (eg, through Paypal)

2.1.3.4 Using in-game mail

- Party A: Selects item from inventory
- Party A: Encloses item in mail
- Party A: Selects mail recipient
- Party A: Sends mail
- Party B: Receives mail
- Party B: Transfers item from mail box to inventory
- Money is exchanged through another channel (eg, through Paypal)

2.1.3.5 Using in-game chat

- Party A: Selects item or bookmark of item and copies to clipboard
- Party A: Pastes bookmark into chat window, IM window, or email
- Party B: Sees item in chat window
- Party B: Selects item to transfer item from Party A to inventory

2.1.3.6 In-game trading tool (eg, Auction House)

- Party A: Selects item from inventory
- Party A: Places it in an auction which includes
  - setting auction time
  - setting buy out price
  - setting minimum bidding price
- Party B: Selects item from auction house interface
- Party B: Decides either on bidding or buying out the item
- Party B: Collects item from mailbox
- Party A: Collects payment for the item from mail box

2.2 Governance

Governance, the means for enforcing policies on players, falls into three main categories.

2.2.1 National law

Some actions or assets in MMO/VWs are covered by national law in certain jurisdictions. For example, under European and US copyright law, it is illegal to show copyrighted movies even inside a MMO/VW. In this case sanctions may be imposed by national courts.

2.2.2 Service provider/ End-User Licence Agreement (EULA)

The EULA is the main instrument of governance used by the service provider. When a user registers, they are bound by its terms as long as they do not conflict with national law. The most important sanction available to the service provider for contravention of the terms of the EULA is the cancellation of the user's account.

EULAs prescribe the rules applicable to access by the user to the virtual world. They should cover key issues affecting the relationship between the owner and the user with respect to access to and participation in the worlds, including:

- The terms applicable to the user's access to the environment.
- Rules governing intellectual property ownership and use, including use of the service provider's intellectual property and whether user content creation is permitted, and if so, upon what terms.
- Acceptable conduct such as griefing and cheating (although this may also be included under a separate set of rules, such as 'community guidelines' or other rules).
- Rules for in-world currency trading.
- The consequences of breach of any of the relevant terms.
- The governing law of the contract.
- Privacy and data handling policies.

2.2.3 Player-to-player

Player groupings such as guilds and clans have agreements (often posted on a guild web site where users can join via a form), which impose certain policies on group members, as well as sanctions on members contravening those policies. Sanctions can include expulsion, downgrading of rank, or an official complaint to the service provider. In theory there could also be a legal contract for such a guild, but we do not know of any groups having legally binding contracts on behaviour.

2.2.4 In-game justice systems

An extension of such governance is the possibility of in-world courts, lawyers and judgements as discussed in (26) and (27). The main sanction available to such a court is an official complaint to the service provider. This also falls under the area of dispute resolution since most cases dealt with (in the few cases existing) relate to disputes between players, rather than violation of a pre-stated policy.

Various experiments have been made with player groupings devoted to resolving disputes and representing player interests. For example, Eve Online players have instituted a "Council of Stellar Management" (28), a democratically elected body which, among other tasks, makes representation to the service provider on behalf of players.

2.3 Scripting features

Scripting is an important source of vulnerabilities. Scripting leads to classic software vulnerabilities but it also provides the opportunity to automate in-world activities and therefore enables potential violations of the game's EULA and disruptions of game play and economics. An example of an extensive in-world scripting language can be found in *Linden Scripting Language* (29).

Important features of scripting languages which often lead to vulnerabilities (with examples of related vulnerabilities in brackets) are:

- Communication with out-of-world network resources (port scanning, DDoS, spam).
    - Http request
    - Remote procedure call
    - Sending email
- Object creation (DDoS, IP related threats)
- Account creation (identity theft, difficulty of detection, attacks on ODR, DDoS)
- Character automation (in-world spam, illegal automation)
- Trading (chargebacks, gold-farming)
- Data collection - in some games it is possible to grab personal data automatically from the game server (see Linden scripting function in *Request Agent Data* (30)).

2.4 Avatar actions and value-transfer possibilities

The following are security-relevant interactions between characters which are covered in some games but not in others:

- Trading
- Killing, fighting, pushing
- Voice over IP with real-world voice
- IM/chat
- Broadcast within a space
- Search
- Cloning of objects and characters
- Teleporting
- Giving
- Showing streamed multimedia content
- Changing appearance
- Physical contact/blocking

2.4.1 Prescripted Chat

Prescripted chat is a mechanism for preventing inappropriate content which is used in many MMO/VWs for minors. Conversation is restricted to a multiple choice interface so that there is no possibility for the users to use inappropriate language. This is used, for example, in the Club Penguin virtual world environment for children (31).

2.5 Game client features

The architecture and features of game clients have important implications for security. These include, for example, the following features:

- **Open or closed source**. Open source clients can be redistributed with Trojans and security flaws. On the other hand, they allow the traditional security audit by the open source community.
- **Data storage and state management** (see (32)). If game clients store state information on the local (untrusted) PC, this leaves open an untrusted machine not only for attacking games but also for attacking the end-user's machine.
- **Credential management**. Where improperly implemented this can lead to identity theft or loss of anonymity. Identity theft can lead to property theft within the virtual world. Project Entropia and World of Warcraft even offer one-time password (2nd factor) based authentication (12) (11).

2.6 Game server features

Apart from vulnerabilities affecting all kinds of servers, there are some game-specific architectural features which can lead to vulnerabilities:

- Whether and how server-to-server and client-to-server protocols carrying game information are encrypted.
- Whether third-party servers are able to provide parts of the world.
- How game time and simultaneity is established.

2.7 Content rating systems

Various independent rating systems specifically designed for games such as the European PEGI (33) and US-based ESRB (34) attempt to rate the content available in MMO/VWs according to its suitability for various age-groups. They categorise content types available within each MMO/VW according to features such as violence, use of profanity, nudity, sexual content, discrimination, etc. All such systems are voluntary but there are commercial incentives to undergo categorisation and the uptake is promising. For example PEGI online, the most active rating system for games in Europe, has rated 9,615 games since its inception (35). An important point to note is that such systems generally only cover publisher-created content. Certain features enable the service provider to influence player created content – for example, guild norms, terms of service, profanity filters and, in games aimed a young children, prescripted chat.

2.8 Age verification

Some MMO/VWs exclude specific age-groups. For example, Teen Second Life is open only to 13-17 year olds, whereas the standard version of Second Life has areas only open to users aged 18 and over. In order to achieve this, some mechanisms must be in place to verify that users are not outside these age-limits – these can range from simple assertion of age to background and documentation checks on registration.

2.9 Automation possibilities

Most games and virtual worlds involve a mixture of human players and automated characters. Automation may be encouraged by game-creators (using scripting, standardized network protocols, etc), eg, to provide virtual employees within Second Life. However (see vulnerabilities) it may also cause problems, disrupting game play and economics. Where game providers discourage automation, there are various measures available to them to prevent characters and processes from being automated within MMO/VWs:

- Server side analysis using pattern recognition algorithms which scan world data to detect automated behaviour and alert system administrators to take action. Using such techniques Blizzard Entertainment, for example, banned 56,000 users who were found to be using the automation software Glider (36).
- CAPTCHAs (challenges based on images containing a text code which is difficult to read automatically).
- EULA clauses forbidding automation.

2.10 Player tracking and behaviour analysis

Many service providers implement extensive mining features within their gaming environment in order to detect anomalous and harmful game-play. This can have privacy implications, as reported in (37).

In-game advertising increasingly uses avatar behaviour to infer the characteristics of the avatar owner for advertising purposes.

Finally, in environments such as Google Lively where world access is directly linked to a broader online identity, in-game advertising can be tailored based on more direct measurements of the user's behaviour outside the world.

2.11 Game culture

Game culture regulates the expectations of the players and therefore what is considered abusive behaviour and what is considered to be valuable in the game. Apart from obvious goals such as entertainment, social experimentation and so forth, which are common to all, games or worlds may be oriented towards different objectives such as:

- Accumulation of wealth,
- Accumulation of social capital,
- Training, or
- Knowledge exchange (business worlds).

What is considered a threat may vary between worlds depending on the prevailing culture. For example, simulation of extreme crimes such as child abuse may be legitimate within a training world designed for police officers to understand and deal with child abusers, whereas within a mass-market game it would be considered as illegal content.

Another important aspect of game culture is the extent to which real-world identity is reflected in the characteristics of an avatar. In a virtual world, identity is much more flexible than in the real-world, allowing easy changes in race, class, gender, age, socio-economic background, and even species. It offers freer self-definition, including multiple identities and shared identity.

Similarly, the originator of a digital persona may deliberately decide to allow his or her avatar to have several "owners" or operators if permitted by the terms of the virtual world.

Some games encourage stable identities (eg, Second Life) where reputation is built up around an avatar. Other game cultures encourage frequent changes of identity and the ability to morph and remain anonymous is an integral part of game-play.

Games also have different cultures around what constitutes cheating and what is considered to be legitimate "gaming the system", the use of offensive language, and sexual content.

2.8 Age verification

Some MMO/VWs exclude specific age-groups. For example, Teen Second Life is open only to 13-17 year olds, whereas the standard version of Second Life has areas only open to users aged 18 and over. In order to achieve this, some mechanisms must be in place to verify that users are not outside these age-limits – these can range from simple assertion of age to background and documentation checks on registration.

2.9 Automation possibilities

Most games and virtual worlds involve a mixture of human players and automated characters. Automation may be encouraged by game-creators (using scripting, standardized network protocols, etc), eg, to provide virtual employees within Second Life. However (see vulnerabilities) it may also cause problems, disrupting game play and economics. Where game providers discourage automation, there are various measures available to them to prevent characters and processes from being automated within MMO/VWs:

- Server side analysis using pattern recognition algorithms which scan world data to detect automated behaviour and alert system administrators to take action. Using such techniques Blizzard Entertainment, for example, banned 56,000 users who were found to be using the automation software Glider (36).
- CAPTCHAs (challenges based on images containing a text code which is difficult to read automatically).
- EULA clauses forbidding automation.

2.10 Player tracking and behaviour analysis

Many service providers implement extensive mining features within their gaming environment in order to detect anomalous and harmful game-play. This can have privacy implications, as reported in (37).

In-game advertising increasingly uses avatar behaviour to infer the characteristics of the avatar owner for advertising purposes.

Finally, in environments such as Google Lively where world access is directly linked to a broader online identity, in-game advertising can be tailored based on more direct measurements of the user's behaviour outside the world.

2.11 Game culture

Game culture regulates the expectations of the players and therefore what is considered abusive behaviour and what is considered to be valuable in the game. Apart from obvious goals such as entertainment, social experimentation and so forth, which are common to all, games or worlds may be oriented towards different objectives such as:

- Accumulation of wealth,
- Accumulation of social capital,
- Training, or
- Knowledge exchange (business worlds).

What is considered a threat may vary between worlds depending on the prevailing culture. For example, simulation of extreme crimes such as child abuse may be legitimate within a training world designed for police officers to understand and deal with child abusers, whereas within a mass-market game it would be considered as illegal content.

Another important aspect of game culture is the extent to which real-world identity is reflected in the characteristics of an avatar. In a virtual world, identity is much more flexible than in the real-world, allowing easy changes in race, class, gender, age, socio-economic background, and even species. It offers freer self-definition, including multiple identities and shared identity.

Similarly, the originator of a digital persona may deliberately decide to allow his or her avatar to have several "owners" or operators if permitted by the terms of the virtual world.

Some games encourage stable identities (eg, Second Life) where reputation is built up around an avatar. Other game cultures encourage frequent changes of identity and the ability to morph and remain anonymous is an integral part of game-play.

Games also have different cultures around what constitutes cheating and what is considered to be legitimate "gaming the system", the use of offensive language, and sexual content.

2.12 User content creation

Not all virtual worlds permit user content creation. Where such creation is allowed, or indeed encouraged, the terms applying to the ownership of the use of such creations must be carefully managed. The key issue is intellectual property, largely copyright and patents.

An issue here may be the use and applicability of Creative Commons (CC) licences, which embed certain terms and conditions on the reuse of the underlying material. CC is actively encouraged by virtual worlds such as SL. The conditions which apply to the creation of objects in SL mirror CC licence conditions, such as "No Copy – Copy" or "Modify – No Modify". These underlying terms will impact on downstream creations.

Further, the ownership of underlying scripts by the owner or third parties, which may have made them freely available, complicates the rights of ownership and use of any creations. Licensing rights will need to be properly cleared. 'Freely available' does not necessarily mean 'free for all subsequent use', particularly where that subsequent use generates a profit.

2.13 Dispute resolution

Policies and techniques for dealing with disputes (Online Dispute Resolution – ODR) can have important implications for security. For example, effective means of recourse can act as a deterrent to harmful behaviour. On the other hand, ODR can be a means to attack other players unfairly. In certain cases, intervention on the part of the service provider may also make them liable to prosecution. In-game courts and judicial processes see [2.2.4] are another form of dispute resolution.

2.14 Financial system

Interesting features of financial systems include:

- **Conversion to real-world money**. Some worlds (notably Project Entropia) have financial systems explicitly based on real-world money, others explicitly forbid any conversion between real-world money and in-world money, while others allow it only through an official channel. In practice, it is very difficult to stop out-of-band transactions since it may be impossible to prove the connection between an in-world transaction and an out-of-world transaction.
- **Credit**. Rules on credit vary between worlds. For example, some worlds allow in-world property to be bought on credit. Banking systems exist in some worlds offering loans in in-world currency. This can create traditional financial problems such as inflation, confidence crises, etc.
- **Chargeback policies on credit-card transactions**. Long chains of dependent transactions can create huge problems when credit card transactions are revoked.

2.15 Access and authorization

Access control in virtual worlds can cover:

- Control of access to areas of the world using automated access control policies applied to areas of virtual space (important, for example, for private corporate zones), or physically using "avatar bouncers" – avatars which physically block entry (or use intimidation to do the same).
- Use of objects – whether a given avatar can use a given object.
- Use of services – whether an avatar has access to a service.
- Access to the world as a whole – whether a character can log in to his or her account. The ability of a given end-user to start-over with a new avatar is an important aspect here. If this is very easy then it is difficult for service providers to block users for violating terms of service.

2.16 Special features of corporate worlds

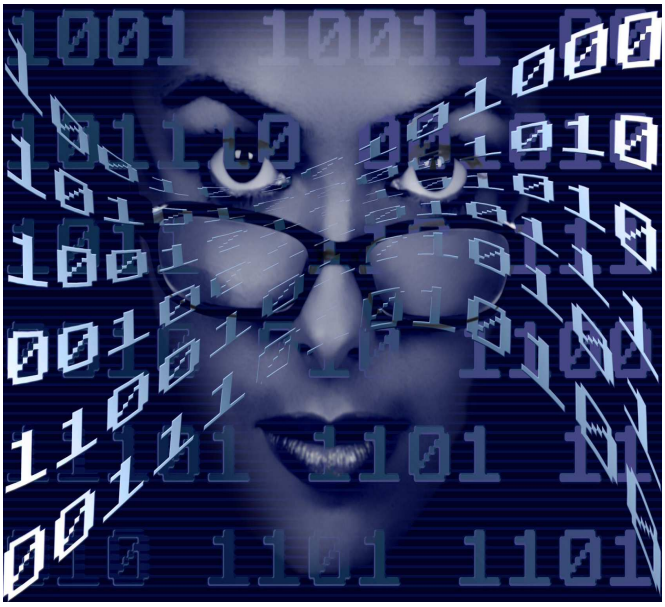
Corporate virtual worlds are a growth area. Gartner estimates that, by 2012, 70% of organizations will have established their own private virtual worlds (38). They can consist, for example, of facilities for meetings (internal or with customers), training exercises (role-based lessons or various simulations), or even of an environment for interacting and working commonly. The main differences from other kinds of MMO/VW are:

- Users can have avatars, but they almost always represent real, known persons.
- Interaction is governed by corporate rules.
- Trading and financial issues, as well as dispute resolution mechanisms, do not exist.
- Authentication is generally stronger, as protected assets are real and often valuable for companies.
- Real-world facilities are contained in the virtual world, eg, document viewers and editors.

The environment of a corporate virtual world can be either the property of the corporation or a separate part of virtual world "farm". Confidentiality, however, is a very important feature. IBM CIO, Mark Hennessey, has stated, "If you really want to make most of these [virtual worlds] meetings, it has to be confidential" (39). Other requirements are for them to be simple and easy to use, with a friendly interface.

3 Principal Risks

This chapter describes the most important privacy and security risks in MMO/VWs. We focus on risks specific to MMO/VWs rather than general information-security threats (eg, identity theft, pharming), unless there is an MMO/VW-specific variant (eg, spam), or a risk is increased or altered by some specific feature of MMO/VWs (eg, profiling). We have followed a typical risk assessment methodology beginning with an examination of the assets under threat. We then list risks by category. The analysis of risks is broken down into assets (the target of protection), vulnerabilities (the technical or systemic weaknesses which lead to the risk), and threats (the potential negative impact).



3.1 Assets

The definition of assets in MMO/VWs deserves special attention. The definition and protection of MMO/VWs in legal and social terms is still very unclear, making them a juicy target for criminal activity. This has led to a strong increase in malware aimed at MMO/VW accounts (see 0 introduction). Already a challenge even in "ordinary" security risk assessment, the definition of assets in MMO/VWs is especially difficult because the objects and services to which value is attached are so different from traditional assets and are without real-world precedent.

The results of the ENISA survey show some examples of typical assets that are considered as such by end-users (18). The particular emphasis on credit is interesting and is perhaps a sign of the times:

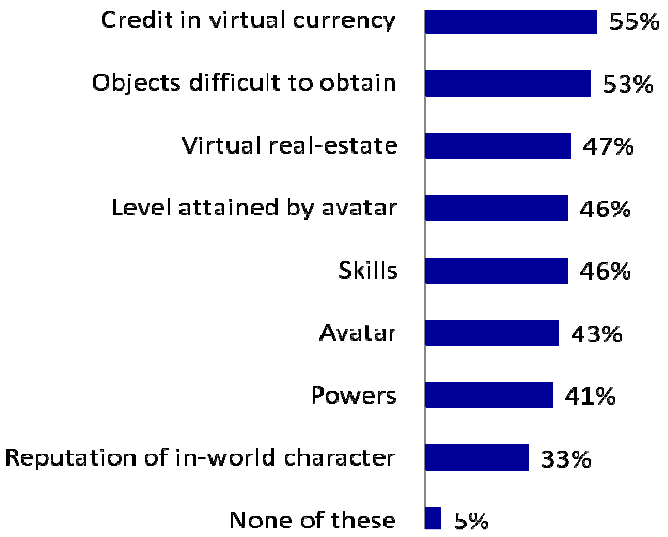


Figure 1:
Items considered as virtual assets by percentage of end-users – ENISA survey data.

Typically the only physical manifestation of a MMO/VW asset is as an electronic record in a database noting how many of a common type of object are assigned to a given player/resident account. This is, however, no different from many other kinds of so-called "intangible" assets (as defined in accounting terminology). Even real money or stocks are usually just an electronic record in a database and assets such as reputation, brand and ideas are equally intangible but regularly incite six-figure law suits.

More important than the fact that they are intangible is that in most game worlds the players have no legal title to the virtual objects according to the EULA and the transfer for external currency is often precluded. Despite this, however, virtual property has considerable value within the global economy. For example, Project Entropia, a MMO/VW where assets and property-rights are well-defined, claimed an annual in-world turnover of US$ 360 million in 2006 (7). The largest segment of the MMO/VW economy takes place outside the allowed limits of the MMO/VW (much of it not officially sanctioned by the world's EULA), ie, on the black market. Total global real money trades (RMT) in MMO/VWs were recently estimated at US$ 2 billion (40). An analyst referenced in a Wall Street Journal article predicted that "non-subscription revenues" from the volume of real-money trades (RMT) on the virtual items market will reach US$5 billion by 2007 (41).

3.1.1 Artificial scarcity

As with any other commodity, the value of virtual property is governed by supply and demand, ie, how much an object or service is sought after and how scarce it is. Scarcity is a very important factor in the functioning of virtual economies. Any bug or loophole in game software which allows "illegal" duplication of assets undermines artificial scarcity and therefore devalues other instances of that asset.

While scarcity of tangible assets is regulated by physical constraints such as the supply of minerals and energy, the availability of virtual assets can only be constrained artificially by limiting duplication of objects in game software and, crucially, by limiting possibilities for automation of tasks (otherwise services become unlimited). This idea of "artificial scarcity" is not new but is in fact central to many economic domains, including the regulation of currency itself – unregulated duplication of cash is probably the oldest form of fraud. It is also a crucial problem in managing the value of assets in areas such as domain names, software and media, where the ability to make unlicensed copies of an asset undermines its market value. In all cases, scarcity is regulated *artificially* by a central authority (in the case of virtual worlds, the service provider or a privately owned in-world central bank).

3.1.2 Intellectual property

In virtual spaces where there is user content creation, the object may be unique and may have a number of properties relating to whether it can be copied, transferred or modified. In games such as Entropia, the object may officially represent financial value that the user has title to, even though the user may not have IP rights to the object itself or access rights to it as such. In spaces such as Second Life the user may have IP rights to the object. However they might not have rights of access to the object. Also, while the object might be exchangeable for external currency, the contract may stipulate that it does not represent any claim to value.

Original works can be created in-world using official tools provided by the service provider (eg, characters in City of Heroes, sculptures in A Tale in the Desert). Even where such tools are not available, original work can always be created in-world. This can be as simple as arranging objects in such a way that they look like something they are not (eg, dead gnomes spelling out a URL in World of Warcraft, or original shapes made from virtual coke cans in The Sims Online). Machinima, computer-generated movies created in real-time using MMO/VW engines, is another example of original work created without the provision of special tools. It is always possible to export content from MMO/VWs. As in all copyright infringement scenarios, a range of tools and capture software exists. Eg, or 3D exports, there are OpenGL sniffers that can construct a 3D model from what the client is told to display by the server.

At the most basic level, copyright also exists in the underlying program, either as a computer program or as a film or audio-visual work, which is possible in some jurisdictions. The tools given to players to create within the world may also be protected

by copyright. When players/residents use those tools to create, they may also bring in third party IP. This means that the end product may be a joint work, the rights to which may be owned by a minimum of three parties, and include potentially infringing material. They may also reproduce real world items in the MMO/VW, such as a painting, building or dress, with consequent potential infringement of underlying copyright and moral rights (the right of authors to protect the integrity of their work). The overlap of contractual rules and general law here is complex.

3.1.2.1 Machinima

Machinima is content which is produced by game players using the game program itself, making it possible for people to produce films at low cost. Increasingly used for non-game related productions, game owners have allowed the production and distribution of such films as a form of promotion of the game. A large number of these movies now appear on YouTube, etc, and there is even a dedicated film festival.

Essentially these films are produced using the intellectual property of the game owner (combined with that of the creator and potentially third parties, eg, music) and are therefore potential sources of dispute over copyright ownership. Whilst no Machinima producer has to date been sued by a copyright owner as far as we are aware, the potential exists for such an action, particularly where the film is disparaging of the game or game owner, contains subversive or offensive content or becomes commercially successful.

Machinima are becoming increasingly sophisticated and are being recognised as an art form in their own right. For more information, see (42). For a further discussion of general MMO/VW IP and copyright issues, see (43).

3.2 Vulnerabilities and threats

3.2.1 Avatar identity theft and identity fraud

The most important security threat to MMO/VWs is the theft of virtual assets using identity theft. The ENISA survey (18) showed that 30% of all users had lost something of value and only 25% of those had recovered the items. The most common way of achieving this is to steal a character's account credentials (username and password) and log into their account. Account information is then used to:

- Sell account for real money outside a VW.
- Sell virtual items for game currency.
- Sell virtual items for real money outside a VW.
- Scam other players.
- Gain access to information about other players (eg, guild members) by posing as another player.
- Damage an avatar's reputation or status within the MMO/VW.

- Damage a person's real-world reputation. It is common to buy and sell "celebrity bodies", whose use within the MMO/VW could be considered libellous and lead to damage of the real-world person's reputation (44).

Account credentials are obtained by the same attacks used to steal any other kind of identity, such as IFrame vulnerabilities (45) (46), and peer-to-peer Trojans (47), although there are some MMO/VW variations on the theme. For example:

- MMO/VW phishing and social engineering:
    - Attacker sends emails disguised as official emails from MMO/VW providers asking for account information.
    - Attacker poses as a MMO/VW provider employee and contacts a player in game asking for account information.
    - Attacker offers spurious in-game rewards to players for which a username and password is required to collect the reward.
- MMO/VW-specific malware:

  Malware refers to programs such as software key-loggers designed (among other objectives) to steal passwords from a user's machine. As well as the typical malware vectors such as p2p networks, some MMO/VW-specific malware vectors include:

    - Links or in-game messages to report updates or patches, which are actually links to malware.
    - Game plug-ins, additional software, or cheats (the latter discourages reporting) that
        - While extracting files or installing, additionally installs a key-logger or
        - Send account information to the attacker.

See references (48) (49) (50) (51) (52) (53) (54) (55) (56) (57).

As well as financial gain, identity theft can also damage reputation in real-life or, more commonly, in-world.

Serious problems can also occur in the relationship between an avatar and their real-world controller.

1. **Masquerading**: Where avatars give information about their real-life (RL) identity, this can be used to deceive other avatar controllers for various malicious purposes. For example, suppose Mallory is playing a female child character and someone says "are you a girl in RL?" or "how old are you in RL?", Mallory can lie about this. Any further references to Mallory's RL are then filtered through this lie. As part of general conversation, he will make up "facts" to cover things that are consistent with being female in RL. In other words, Mallory constructs a completely fictitious other person. He is no longer role-playing a female character, but role-playing a female player role-playing a female character. He may even build an out-of-game presence on a social network or a blog to add weight to the persona. While the consequences of this are in most cases entirely harmless (and part of the enjoyment of the game), it can lead to issues such as child-grooming and other serious issues if characters meet in real life.
2. **Lack of accountability**: False details given at the registration phase of any MMO/VW make it difficult to hold users to account for malicious behaviour in-world.

3.2.1.1 Targeted attacks on guild banks using identity theft

In games such as World of Warcraft, in-game guilds have banks where they store their most valuable items. Full access to such guild banks is limited to players high in the guild hierarchy. However guilds often have web sites open to guests where information such as email addresses, instant messaging usernames and social networking details, are available. Members of the guilds are also active in forums. This leads to the following attack scenario:

- Attacker visits guild sites or forums and checks in the MMO/VW to gather a list of high-ranking officers in the guild and their contact information.
- This is used to gain account information that can be used for social engineering, phishing, hacking, etc.
- Attacker logs in as a player, accesses guild bank, and sells all items.
- Attacker changes account details so a player cannot login.

3.2.2 MMO/VW Privacy Risks

Although it is conceivable that one day a declaration of Avatar rights – some already exist (58) – might claim an inalienable right to data privacy for avatars and that the avatar's consent must be obtained for any data collection, this seems far-fetched at the moment. The European Privacy directives certainly do not apply to avatars – as distinct from their owners. Nevertheless the privacy of the *avatar controller* is a very important issue which is often overlooked.

Representation as an avatar is little different from using any other form of online persona – users are free to present as accurate or inaccurate a picture as they choose. There is a spectrum of self-representation in MMO/VWs ranging from accurate portrayal of the avatar controller, mirroring their real-world persona to fantasy characters who behave entirely differently and give the controller the opportunity to escape their ordinary persona. At the self-representation end of the spectrum are MMO/VWs such as Kaneva and Google Lively, which may be seen as 3-dimensional versions of social networks or chat-rooms. In such MMO/VWs, users tend to give away significant sensitive personal information. Because avatars give an illusion of anonymity to interactions, there is even a tendency to give away even more sensitive personal data than in a "traditional" social network. Where personal data about the avatar controller is disclosed, European Law certainly applies, since it covers the processing of personal data which is defined as:

> "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*;" (59)

Even in game worlds, where the tendency is more towards fantasy personalities than self-representation, certain characteristics of the avatar owner can be guessed with reasonable accuracy based on statistical analysis. For example, a survey of the 2001 fantasy game Everquest showed that only 2.5% of female users and 15.7% of male users had played characters of the opposite gender, ie, if an avatar in this game is male, his owner is at least 97.5% likely to be male (or more, since the number of male players is usually greater than the number of female players) (19). The inclusion of IRC and VOIP channels in MMO/VWs leads to significantly increased disclosures of private data, such as location and personal characteristics, through voice and use of language.

In practice, bulk data collection, including the collection of personal information, occurs in MMO/VWs for the following purposes:

- Improving game-play based on in-game statistics.
- As anti-cheating measures. An example of this is Warden, a component of World of Warcraft's client software, which is aimed at detecting violations of their terms of service (60). The software sends information back to the service provider on activity on the local machine and has many features in common with spyware programs (eg, polymorphism – aimed at avoiding circumvention by cheats).

- To protect of minors. Service providers may pay particular attention to monitoring and detecting behaviour which threaten minors.

- Marketing (in-game or out-of game). A privacy-related feature peculiar to MMO/VWs is the ability to eavesdrop. Privacy tends to be a function of proximity in most virtual worlds, so in most worlds any avatar or object has access to conversations and activity taking place within a certain range of virtual space. There is usually no possibility to limit this feature except by explicitly "whispering" in the case of instant messaging or VOIP. This opens up various possibilities for privacy invasion. For example, some companies are already offering in-world behavioural marketing services based on eavesdropped conversations.

  > "*A ContextAds board listens to the conversations of those avatars around it, displaying advertisements when certain keywords are mentioned. Advertisers can bid on keywords, with their account only being charged when their ads are actually shown. Avatars can click on advertisements of interest to them, and can be offered a website or a teleport to an in-world location.*" (61)

  With in-game advertising revenues growing exponentially (62), this is likely to become an increasingly important issue.

- To gain advantage in the game or the game economy. Having more information about other users in a world can only be an advantage. Using proximity-based eavesdropping in conjunction with a centralized reporting system, it is theoretically possible to set up a virtual "spy network" in most virtual worlds, giving the controller unfair advantage in the game or game economy or providing them with statistical data which might be used for in-world or out-of-world marketing. Services already exist which aggregate player information, eg, Thottbot in World of Warcraft (63).

3.2.3 Automation attacks

Service providers encourage some forms of automation such as automated staff for an in-world service or smart user-created objects, eg, musical instruments. Other forms of automation are however very problematic for service providers. In fact most MMO/VWs can only survive if certain activities are restricted to humans.

A typical example of the exploitation of MMO/VW by automation is the Glider application used in World of Warcraft (64). This reference describes Glider as follows:

> "*Glider is an application that permits WoW users to automate game-play. Because Glider does not eat, sleep, go to work or attend school, it can control a player's WoW character all day and all night, all the while accumulating virtual wealth and experience points for the player that uses it.*"

Some forms of automation allow attackers effectively to obtain objects or services "for free", ie, without the expected effort which gives them value. This leads to the deflation of their in-game value for other users. Critical activities of this type include:

- Economic transactions – the ability to trade automatically gives the bot controller advantage over traders who have to "work" for profit.
- Performance of valuable services or repeated actions which accumulate value and which most avatars cannot automate. This again effectively gives the bot controller free access to an asset of value within the game (sometimes known as gold-farming).
- Gaining status in a way which is difficult for a human-controlled avatar. If it is possible for a bot to increase the level of an avatar in a game (power-levelling) then this service (which is effectively free for the bot-owner) can be sold to other players.

Automation can also be used to corrupt game-play or circumvent rules and restrictions. Critical activities of this type include:

- Customer-service and dispute-resolution requests – these can be used to perform DoS attacks on MMO/VW providers (flooding their ODR systems with requests).
- Tele-hacking – moving avatar locations in ways which are not possible through a standard user-interface.
- Account creation – this can be used to avoid bans for violating terms of service or to exploit free trial periods.
- Attacks against probabilistic in-game bugs (eg, duping bugs often can only be made to work one time in a hundred, or less often – using a bot allows "brute-forcing").
- Killing and damage to other characters where most other avatars cannot automate – gives unfair advantage to the bot-owner and disrupts game-play.
- Co-ordinated operations involving multiple automated avatars, eg, in-world flash crowds.
- Collecting and sharing of data about other avatars or their controllers using "access-by-proximity". This violates privacy and can be used to gain unfair advantage in game-play by "omniscience" not available to other avatars. For example Thottbot collects information about World of Warcraft players (65).
- Collecting and sharing of data about economic variables, eg, auction prices. The data can be used to gain unfair advantage in game-play through "omniscience" not available to other avatars. (This is comparable to insider trading in real-world economics.)

3.2.3.1 Possible threats from Scripting languages

Scripting languages, such as Linden Scripting Language (LSL) (29), are used to automate operations. Certain features of such languages are particularly vulnerable to exploitation:

- XML Http and RPC requests can lead to spamming and port scanning.

- Duplication of objects. Any function which allows objects to self-replicate opens up DoS vulnerabilities.
- Data collection functions, such as LlGetLandOwnerAt in Second Life, which allow harvesting of personal or economic data, can lead to privacy threats and attacks on the economic system.

3.2.3.2 Security and privacy issues connected with combating automation

Attempts to combat automation carry their own security and privacy problems. Often the only way to detect automation is by analysing large amounts of potentially sensitive data both from the SP's own databases and from the user's machine. (Some attacks intercept and inject network packets exchanged with the client in order to automate processes.) Perhaps the most well-known case is WoW Warden (66), a module which aims (among other things) to prevent automation-based cheating in World of Warcraft. In order to do this, it employs many of the same tactics used by spyware programs:

- Polymorphism – the software attempts to avoid detection. See (67).
- Phoning home – sending data about the user's machine back to the service provider to analyse behaviour.

3.2.3.3 Gold-farming by humans

Gold-farming refers to professional operations aimed at accumulating value in MMO/VWs, usually through repetitive actions. It may use automation, but it is also common for such operations to use cheap human labour instead of bots. Gold-farmers are low-paid professionals who spend their working hours playing MMO/VWs in order to gain objects or characters of value and sell them to players who do not have time to earn them. Gold-farming in China takes place in "sweat-shops" where working conditions are very poor and comparable to clothing sweat-shops, hence the analogy. A recent lawsuit brought by a user group against IGE, a provider of virtual assets, some of which are produced by gold-farmers, illustrates the disruptive effect this activity can have on other players (68)).

3.2.4 Cheating, security issues

What constitutes cheating and what is simply a clever tactic for gaining advantage in the MMO/VW is often a matter of debate. As an illustration, (69) reports that Zhou Xujun, who was banned from World of Warcraft by The9 (who operate Warcraft in China) for what they consider cheating, had the ban overturned. Behaviour which some players may consider legitimate will often be considered cheating by service providers if it disrupts the functioning of the game and/or its economic system and causes players to leave. Many players consider that any tactic which is not prevented by the game software itself is legitimate. This leads to an arms race of exploits and patches.

We now describe some important examples and categories of cheating. Illegal automation is a form of cheating which is considered in depth in [3.2.3].

3.2.4.1 Duping

Duping refers to the exploitation of any feature of a game to duplicate objects of value in a way which was not intended by the game provider. This may be compared by analogy to the counterfeiting of real-world money. Games are designed so that objects of value maintain a certain scarcity, but if a player can create more than the intended number of objects or create objects with less effort than intended, that player gains an advantage and all other instances of that object are devalued. Duping becomes cheating when players deliberately attempt to leverage it instead of filing bug reports.

State-management vulnerabilities

Most duping happens as a direct result of bugs in the server logic for the handling trading of items between users. This is because tracking the number of instances of a certain object type requires three separate remote computers (person 1, person 2, and the server), all of which have latency, packet-loss, and connection-loss to deal with, so there are many complicated failure modes. It is very challenging to enumerate all of them and deal with all of them correctly. Also tracking instance numbers requires the simultaneous updating of database records on distributed database servers as well as distributed connection-servers (with IP connection to the clients).

MMO/VWs typically have to maintain a game or world state shared over the Internet between hundreds of thousands of clients and hundreds of servers. This introduces many vulnerabilities where failure modes of state management can be attacked. Online Games and Security (70) even claims that "*race conditions* (71) *… and other problems with state are the primary source of bugs in online games*".

In systems where critical operations are divided into transactions handled by multiple servers, vulnerabilities can often be exploited by interrupting such a transaction in mid-transaction. For example, suppose player A gives asset C to player B just before player B crosses a server boundary. At the same time, player A forces a log-out or performs a DoS attack using a botnet on the server he remains on. This can cause a failure of an attempt to remove C from A's inventory so that the asset is effectively duplicated.

Such bugs can have very serious consequences. For example, a bug in 2005 in the game Everquest II resulted in a 20% inflation of the game economy in just 24 hours (72) (73). Other examples of attacks exploiting such bugs can be found in (74) and (75).

3.2.4.2 "Insider Trading" (gaining economic advantage using information not available to other players)

The recent case of *Bragg-vs-Linden* (76) is an interesting as it concerns a dispute between the service provider and the user about what constitutes cheating. Marc Bragg purchased land via auction pages which were not officially public but nevertheless available online by appending an easily guessable ID number to the auction URL. Linden claims that Marc Bragg gained unfair advantage by accessing land auction pages for Second Life property that had not yet been officially released for auction, enabling him to acquire land in Second Life below Linden Lab's cost for that land. (He paid only US$300 for an entire region.) Linden Lab suspended Marc Bragg's account for investigation and then closed the

account for violation of its terms of service and dissolved his virtual assets, Linden Lab's usual procedure for closed accounts. Bragg declared that his actual losses were between US$4,000 and US$6,000. The arbitration clause in the ToS was held to be unenforceable on the basis that it was unconscionable and the matter was ultimately settled by the parties.

3.2.4.3 Induced Suicide

An example of a common scam which is considered by most players and service providers to be cheating is inducing a victim to commit suicide so the "corpse" can be looted. Various Windows key-presses cause character suicide in some games, especially Alt-F4 in web browser games. An attacker may therefore lure a victim to a remote location and tells them to press Alt-F4 to "enable cheat mode" or some other spurious "secret benefit". For example, the attacker might offer to trade or gift a high value item, but doesn't press OK, and claims in chat that the chat window "is broken". He then tells the victim to press Alt-F4 (a suicide key-sequence) or something similar.

3.2.5 Harassment

In-game verbal and sexual harassment can be just as serious a threat to real-world people and resources as any other kind of online harassment. Harassment threatens end-users by causing emotional distress and disrupting or interrupting their experience. This in turn threatens game providers by reducing user numbers, revenues and reputation. It can also have this effect indirectly by downgrading the quality of the culture present in the world, causing players who are not themselves victims to cancel subscriptions.

As part of a campaign by another user, the victim of harassment may also be made accountable for infringements for which they were not in fact responsible (ie, by false reporting to online dispute resolution systems) and may have their account unfairly cancelled. Users may also find their reputation or that of their avatar (in- and out-of-world reputations) can be damaged by concerted campaigns. The fraudulent use of online dispute resolution mechanisms is also a serious waste of the provider's resources.

There are three main forms of harassment:

3.2.5.1 Character related harassment

- **Ganking** (see Terminology and Abbreviations): an avatar is repeatedly killed by a malicious party. This can happen if:
    - Party B waits for Party A to resurrect or reappear in a certain place,
    - Party A is much weaker than Party B, ie, is a lower level character,
    - Party A has very little or no chance at all to defend itself, or
    - Party A is unable to continue with playing.
- **Kill stealing**: a party starts the encounter and when they are almost done, another party finishes it taking credit for the kill. See, for example (77)

- **Ninja looting**: players in a group have arranged in advance to share out the spoils a certain way, but one of the players takes something they were not supposed to get.

- **Party A kills Non-Player-Characters** (NPCs) needed by party B to complete an in-game task, even thought Party A does not need them. Party B is unable to proceed with the game.

- **Griefing** [see Terminology and Abbreviations] attacks on players. For example, in Second life it is possible to push another character and prevent them from performing actions in the world. For example avatar A might push avatar B off the stage during a public performance.

3.2.5.2 Verbal Harassment

Verbal harassment can be a problem particularly when aimed at minors. It can happen through any of the following channels available in-world:

- Chat (offensive content or text links to web-hosted offensive content),
- Voice over IP,
- Images embedded in chat channels,
- Sending an in-game item link to a user-generated item that contains offensive text or images,
- Depositing user-generated items in the vicinity that contain offensive text or images,
- Re-arranging items in the world to "spell out" an offensive message:
    - For example, in World of Warcraft, creating a new character, moving it to a location, and then making it commit suicide, leaving a corpse. This way, done fast enough, you can spell out a message. Usually this is used to spell out the URL of an illicit gold-farming or RMT site. There are many examples on YouTube, etc.

Insulting or offensive content can include:

- Inappropriate comments and proposals of a sexual nature.
- Referring to sexual acts with minors, animals, or sexual violence.
- Abusive, violent or offensive language.
- Real life threats.
- Inappropriate comments related to a person's beliefs or religion.
- Racist and nationalistic abuse.

3.2.5.3 Reputation related harassment

Another class of harassment-related threats are directed at deliberately damaging a user's reputation (in- and out-of-world). This tends to be a more important issue than in the Internet at large because attacks on reputation may be seen by many players as simply

another legitimate tactic to gain advantage in the MMO/VW. This can happen in various ways:

Reputation damage through identity theft

A typical scenario is:

- Party A acquires Party's B account and poses as that player
- Party A scams and cheats other players
- Party A acts in a way that will ruin Player B's reputation – offends others, posts inappropriate content, etc. OR
- Party A gains steals assets of Party B (eg, from guild bank) - Player B is held responsible for that action.

Offensive Posting

Party A posts offensive, false information about Party B either on game MMO/VW related forums or in the game itself. Note that the attacker will usually take steps to ensure that messages are NOT read by the victim.

This might, for example:

- Cause a player to be rejected from groups or guilds thereby disadvantaging them in the game,
- Disrupt any trade or exchange of assets due to a poor reputation, or
- Cause a Guild whose reputation is being lowered to have problems acquiring members.

Abuse of Online Dispute Resolution

- Party A provokes Party B, and then
- Party A pre-emptively complains to in-world support or out-of-world support that Party B is harassing Party A, in an attempt to have Party B's account cancelled or otherwise damage their reputation.

This is often done using a throwaway account, so that if Party A is held to account, they can just cancel the account and suffer no damage.

3.2.6 Trading and financial attacks

3.2.6.1 Credit card chargebacks and payment reversals

Whenever a purchase is made with a credit card, or other online payment facility, a full refund can be claimed from the payment company within a certain time limit (usually 1 month) if a complaint is filed. The payment company then claims the money back from the retailer. In most cases, the retailer is presumed guilty, and it is hard and convoluted to contest the chargeback. When a chargeback happens, retailers lose money - *even if* the

consumer has already made full use of the service they paid for (eg, if the payment was for a subscription). Payment companies tend to be especially willing to reverse payments made for goods purchased in MMO/VWs – in some cases they have a specific policy of allowing the reversal of MMO/VW payments no matter what the claim, but not a similar policy for real-world purchases.

Worse still, CC and payment companies monitor the volume and frequency of chargebacks issued against a particular provider. The more chargebacks are attached to a particular vendor, the more money the credit card company charges the retailer as its commission on ALL payments (even legitimate ones). Thus the provider's profit margin reduces when the number of chargebacks it experiences increases.

It is relatively easy to purchase tens of thousands of valid CC numbers from illegal sources. If a credit card number is used fraudulently, there is often no information about who is actually using the service or goods. Even the originating IP address can be obscured relatively easily using public proxies, zombies or anonymising services (or a combination of all these).

Types of Attack

Against the MMO/VW provider:

- Pay for game for 30 days, then issue a chargeback and effectively "play for free". This can be repeated every month, until the company successfully challenges one of the chargebacks.
- Pay for items in-world, use them for a while, and then issue a chargeback. This is effectively a "try before you buy", except that the company suffers additional loss with the CC processor.
- Purchase-then-refund using credit card chargebacks:
    - Attacker makes high-value purchase in-world using a credit card (stolen or otherwise),
    - Attacker resells in-world items, and
    - Attacker waits two or three weeks and then initiates a credit card chargeback via his or her credit card company.

This is especially damaging with extremely high-value items or where extremely large numbers of follow-on sales are possible. For instance, in Second Life, it is possible to spend tens of thousands of dollars on a single purchase and then to split a single plot of land into a large number of sub-plots which are then sold on to many people. As a result:

- The original retailer has given away high-value item for zero money.
- The original retailer may not be capable of redacting the transaction for the in-world items, especially if in-world trades are non-reversible as a result of out-of-world trades.

- The attacker may sell and re-sell in-world products through a chain of accomplices and some non-accomplices in order to launder them in case the world-owner attempts to selectively reverse-out the trades. As a result, the world-owner is now aiding and abetting money-laundering. Note that the attacker is willing to make a net loss in these transactions in order to launder the money. Note that laundering real-world money in this way is at present a theoretical attack since there is no data on actual occurrences.

Another possible attack is to use a credit card chargeback to extract real money. By combining the money-laundering approach with the stolen credit card:

- Attacker uses stolen credit card to purchase something in-game.
- Attacker sells item to other player(s).
- Attacker "cashes-out" the in-game credits for real-world money. In games that allow for direct RMT (real money trades) cashing out could be via a world-owner approved or owned marketplace. In games in which RMT is illegal, it could be through selling things out of band, eg, on eBay. With out-of-band sales, the MMO/VW provider has the difficult choice of confiscating the goods from the new owner or accepting the loss of money.
- Attacker issues chargeback.

3.2.7 Risks to intellectual property

Risks associated with the use and creation of intellectual property in world can arise from the user's misunderstanding of the terms of service (ToS). The nature of the actual rights held by the user is invariably only vaguely defined. The situation is complicated by a layering of rights (as described in [3.1.2]) and the large number of users involved in the creation and participation in such environments. It is also complicated by the differences in national laws regarding the scope and nature of copyright protection.

Users often wrongly assume that they are protected by the intellectual property laws in force at their place of physical origin. The terms of service may grant ownership of intellectual property to the user *along with* a royalty free licence to the owner of the virtual community. Even then, there may be a mixture of user generated content and content provided by the service provider, eg, textures in Second Life are often owned by Linden but may be used to create objects of IP which are officially owned by the end-user. In other words, users' original work may be composed using underlying visual works in which copyright is owned by the owner of the virtual world or by other users of the world. Indeed a creation may combine the intellectual property of multiple users.

From the user's perspective, the only relevant 'property' is the end product: the dress, the sword or the car, and not rights in the underlying code. However, unless the underlying code is transferable the property itself will not be transferable, thus reducing its value and rendering the grant of intellectual property rights meaningless. Rights may also subsist in any design, drawing on work produced as part of the process of development. Service

providers may purport to grant IP rights to users, but what these actually consist of is extremely vague – certainly something less than outright ownership.

The outcome of the litigation in *Blizzard v Glider* (78) is relevant here. Blizzard, the owners of World of Warcraft (WoW), claimed *inter alia* that Glider, through the manufacture and sale of Glider, was liable for the contributory and vicarious infringement of copyright in the WoW software, by facilitating and encouraging the direct infringement of copyright by users of WoW in conjunction with Glider. The judge held that use of WoW is governed by two agreements, the EULA and the TOU. Blizzard had structured these agreements to make it clear that all use of the game software is subject to compliance with both the EULA and the TOU. The judge held that this meant that the license to use the game software was limited by these conditions, making any use of the software *in breach of the provisions* outside of the scope of the copyright license and not merely a breach of the contract. Section 4 of the EULA, which included prohibitions on copying or modifying the Blizzard software, was found to limit the scope of the license granted to users. Therefore, the court held:

> "*Users of Glider clearly violate the prohibition in section 4(B)(ii) of the TOU against the use of 'bots' or any 'third-party software designed to modify the [World of Warcraft] experience.'... Players who use Glider to mine WoW for game assets also violate section 4(B)(iii). When WoW users employ Glider, therefore, they act outside the scope of the license delineated in section 4 of the TOU. Copying the game client software to RAM while engaged in this unauthorized activity constitutes copyright infringement.*"

This decision is important for the recognition of the power of the EULA in modifying and regulating the grant of the copyright licenses, which are dependent upon the particular drafting of the WoW EULA and TOU. Note that the Digital Millennium Copyright Act (DMCA) claims relating to circumvention were largely left to be dealt with at trial.

3.2.7.1 Third party theft of intellectual property

Where content may be created and traded for value, it may also be copied. Linden Labs experienced the problem of the "copybot" (79), a third party program intended to enable inventory backup, but used by third parties to copy vendors' commercial products without permission. More recently, technical glitches have allegedly been used to facilitate unauthorised copying of items tagged as 'no copy' and resale of those items. This copying of virtual items is copyright infringement.

Service providers may wish to distance themselves from these disputes between users by relying upon procedures such as the safe harbour notice and take down provisions under the DMCA (US) (80). However, the scope of the DMCA has yet to be fully explored judicially. The equivalent legislation in Australia, for example, is much narrower in application and it is likely that a service provider would not fall within the protective scope of the legislation, leaving the owner potentially liable for authorisation liability or even direct infringement.

3.2.7.2 Avatar names and identities

Ownership of avatar names and identities is also problematic, giving rise to issues of trade marks, misleading and deceptive conduct, as well as issues of publicity rights. In Second Life (and other civic or social worlds) the choice of avatar name may be restricted, either due to guild or social status or because of a finite list of names. It is not clear if the creator owns the rights in their avatar name, particularly if they want to exploit that name outside the originating MMO/VW.

3.2.7.3 Brand control

Owners of virtual worlds may need to monitor and control use of their trade mark and identity by third parties, including logos and even character and guild names. Second Life has recently created clearer rules on the use of its name and logo by third parties. There is also the issue of the use of existing trademarks and trade dress within virtual worlds, often as a form of tribute or homage; see the *DC Comics* case (81).

3.2.7.4 Copyright violations by end-users

As with other internet media where users may contribute content and media, users of MMO/VW often import copyright and trade mark material without the permission of the copyright owner, which may or may not be required. For example, although this is not sanctioned by the terms of service, users may display copyrighted movies within Second Life spaces.

As noted above, although service providers may seek to distance themselves from infringements committed by users, there is still a real possibility of liability for copyright infringement on the basis of inducement, authorisation or vicarious liability.

3.2.8 Information security related risks for minors

Minors can be exposed to inappropriate content in MMO/VW environments either through circumvention of age-verification techniques or through the failure of content rating systems. When this happens, they may be exposed to the following types of harmful content.

- Disclosure of real-world contact information.
- Bullying or humiliating messages damaging the reputation of the minor.
- Pornographic or violent images or any content which does not match the rating of the game.
- Offensive language.
- Breaches of privacy. Online game-play sometimes encourages children to build relationships, share personal details, or even meet unknown fellow players outside the game.

- Content with rules or awards deemed inappropriate (eg, high-value prizes).
- Content being created as a result of the game which could be unsuitable for young people and a mismatch with the rating given for the game.
- Some players engaging in behaviour that might not be suitable for young people. Examples would include inappropriate or offensive language, bullying in games that allow text, voice or video communication, unsporting conduct like cheating and tampering, or aggressiveness towards others.
- Links to websites where content may not be suitable for young people and that use phishing techniques to persuade them to follow the links.

3.2.8.1 Age verification

Age verification techniques range in strength from:

- simple "click-through" agreements which require the user to state they are over 18 through,
- email accounts issued at birth by government agencies which can be used to verify age, to
- the use of electronic national ID cards (smart cards) underwritten by governments whose possession is proven by a PIN or password.

The key elements of a workable age verification solution are:

1. **Government underwritten registration procedure**. Registration and enrolment must be carried out by trusted personnel, without commercial motivation to fraud.

2. **Strong proof of possession**. It should not be possible for anyone except the person issued with the authentication token or secret to use it. Passwords are one solution here but people (especially minors) often give away both their token and its password to another party. One partial solution is to use the disclosure of more sensitive data as a disincentive to password delegation. For example the use of a secure email address issued at birth has this effect because delegating a password would give access to all the user's mail. On the other hand this makes the damage much greater if it does happen.

3. **Inexpensive**. Placing fingerprint readers in every key of a keyboard so you can see who is typing every key is possible, but prohibitively expensive (and a serious invasion of privacy).

4. **Convenient**. One way to get round age restrictions would be to remove home access to the Internet and force users to use certified work spaces if they wanted to use the Internet, but this would be too inconvenient.

5. **Not intrusive**. Making people wear brainwave-scanners or have RFID chips in their hands would work, but is too intrusive.

We note that verifying that some-one's age IS greater than 18 may be easier than verifying that their age is less than 18, as there are a larger number of other use-cases which require proof of majority and there are also a number of documents, such as driving licences, which are only available to people over a certain age.

It is the opinion of this group that no currently available technical age-verification techniques can satisfy the above five requirements for remote age-verification. Electronic ID cards can be delegated (experience with credit cards shows that people will delegate even highly sensitive tokens), click-through agreements provide no assurance, and email addresses can be attacked with phishing. Passwords can be delegated resulting in even more serious damage. See the recommendations [4.3.2] below for further discussion.

Despite this, the ENISA survey showed that 53% of users were willing to trust the effectiveness of age verification schemes (18).

3.2.8.2 Weaknesses in Content-rating Schemes

Effective content-rating systems are particularly challenging within MMO/VWs because a significant proportion of the content is not determined by the service provider but by the end-users participating in the game. Therefore any assessment of the content of a MMO/VW is dependent on:

- The game culture (see [2.11]) prevailing at the time of the assessment. This culture may change over time or even vary with the time of day.
- The effectiveness of identity and age verification procedures. Vulnerabilities in age-verification can, for example, allow adults to enter an environment which has been assessed on the assumption that it is only accessible to users under 12.

Despite this, the ENISA survey results showed that 51% of users were willing to trust the effectiveness of content rating schemes (18).

3.2.8.3 Prescripted Chat

Prescripted chat (where conversation is restricted to a multiple choice interface) has several weaknesses in its implementation:

- Providers often give an override facility under certain circumstances which allow malicious parties to abuse this feature (eg, if the other party has been authenticated – but not strongly).
- Choices can be used as part of a pre-agreed code-language to transmit inappropriate content.

3.2.9 Problems with Online Dispute Resolution in MMO/VWs

In 2006, Second Life received 2,000 ODR requests per day (82). As its peak number of concurrently active accounts at that time was only approximately 30,000 (83), this is a very high number, although it is typical for virtual worlds. The prevailing culture of many MMO/VWs is that anything which is allowed by software is acceptable as a means to gain advantage in the MMO/VW. If ODR requests can be used to gain advantage over other avatars, using them is considered fair play by many users. This is an important contributory factor to what is essentially a break-down in the ability of many SPs to deal with the number of complaints received.

Typical risk scenarios may be:

Scenario 1

- Player A makes a false complaint about another through the in-game messaging system.
- MMO/VW representative (a Game Master or GM) contacts Player A.
- Usually using standard scripts, the GM quickly identifies the problem.
- GM contacts Player B against whom the complaint was filed.
- Player B is advised to refrain from that behaviour.

Scenario 2

Party A provokes Party B, then pre-emptively complains to in-world support or out-of-world support that Party B is harassing Party A, in an attempt to cast suspicion on Party B's activities.

Scenario 3

As above, but using a second attacker account, Party C, to provoke Party B, so that Party A benefits when Party B gets banned or logged out, even if Party C is later penalised. The most common result of such attacks is the temporary removal of competitors from an area, as often Party B will get a "gentle warning" ban for an hour or a day.

Scenario 4

- Player A reports Player B for naming his character, items, etc, in a way that offends Player A or is against naming rules. The name does not even have to be inappropriate in a language that is used in the MMO/VW.
- GM contacts Player B explaining the complaint and asking him to change the abusive name.
- Before logging in to the MMO/VW Player B is prompted to change the abusive name, thereby losing accumulated reputation.

Scenario 5

- Player A reports that his account is being hacked and all his items stolen (in cases where the account details were not changed and player still has access).
- Player A is asked to provide data needed for ID and account confirmation.
- MMO/VW provider starts remediation process and
    - Player A receives all his items back,
    - Player A receives items with a lower value, OR
    - Player A receives all his items back but since they were sold in-game, he needs to repay the value so as not to disturb the game market.

3.2.10 MMO/VW spam

Another issue related to harassment is MMO/VW spam. Many bots (scripted avatars) exist within MMO/VWs, and these bots peddle the usual spam-ware content of:

- Unsolicited marketing (which is outlawed by EU directive 2002/58 (84))

Offering or advertising services or products banned or not allowed by the MMO/VW provider (eg, gold selling in World of Warcraft).

3.2.11 MMO/VW specific Denial of Service attacks

Denial of Service (DoS) attacks aim to render an application or application feature incapable of providing normal service. Virtual Worlds are especially vulnerable to DoS attacks because they generally have a centralized architecture and are accessed from a large number of poorly authenticated clients. Changes affected by one client are often transmitted (by virtue of the shared and persistent nature of MMO/VWs) to many other clients. While traditional DoS attacks are usually financially motivated, MMO/VW DoS attacks may additionally be used to gain advantage in the game (and possibly as a result also of real-world financial advantage). This expands the range of DoS attacks attractive to attackers. DoS can affect MMO/VWs through the following vectors:

3.2.11.1 Distributed attacks on network and processing resources

Because subscribers pay monthly subscription fees for access to many MMO/VWs, downtime can cause substantial losses for service providers. Reports of attacks, such as those mentioned in (85) and (86), suggest that there is a serious possibility of organized Distributed Denial of Service (DDoS) attacks being used to blackmail MMO/VW service providers. This is similar to the increasing number of DDoS attacks being made against more traditional targets such as banks, payment gateways, and online gambling sites.

Resources vulnerable to DDoS attacks are bandwidth for communication and storage of world data as well as computational power to process all the simultaneous actions used in the virtual world. Short outages of one or more resources, or peaks of the system's usage, can prevent a service from being delivered properly. For example, in 2006, Internet service company Netcraft documented downtimes in the World of Warcraft network (87), which were allegedly caused by network problems of the ISP hosting the application.

3.2.11.2 Object creation

Scripted objects in MMO/VWs open up several possibilities for a single user to create a DoS attack. The main vulnerability is the ability to create self-duplicating objects or avatars which can create unlimited object instances. This allows a single player to fill virtual spaces with a certain object, thereby blocking "physical" access by other avatars and creating excessive load on any servers dealing with their representation. Publisher Linden Lab needed to temporarily shut down its system in the past to combat new malicious objects (88). Attackers exploited the system's flexibility by creating self-replicating objects, causing a logical time bomb in the servers.

3.2.11.3 Avatar interactions

Various avatar actions (see [2.4] above) are vulnerable to DoS attacks. In this class of attack, avatar A interacts with the game environment, non-player-characters (NPCs) or other players, in order to prevent another avatar from continuing with the game or otherwise disrupt the other avatar's game-play. These interactions might include:

- Constantly interacting with NPCs so others are prevented from doing so.
- Blocking access to different locations or areas. An example of blocking behaviour, which effectively amounts to denial of service for other users, can be found in (89). This example is from Dark Age Of Camelot – where avatar A stands on a bridge blocking other avatars from crossing that bridge without being hit by avatar A. Technically the player does not contravene any rules or terms of the EULA, yet this tactic ruins the game for others.
- Repeatedly opening the trade window with a user, causing pop-ups to appear on their screen and obscure their interaction with the MMO/VW.
- Interacting with the world in such a way as to manipulate the world-logic into harassing the victim, eg, by attracting the attention of a powerful monster and leading it to other, probably weaker, players who get slaughtered.

- Attempts to get an avatar banned by reporting to ODR systems.

3.2.11.4 DoS Attacks on game clients

If too much information about an avatar is revealed to other users (eg, the IP address), this can be used to perform DoS attacks on the client. Another approach to attacking a single client is to flood them with messages via the built-in communication system of an MMO/VW. Many ingoing instant messages or voice-over-IP requests can prevent the user from performing their intended actions.

3.2.12 Malicious game servers

Although MMO/VWs suffer far less from piracy than single-player games, the server software does occasionally get stolen. Rogue servers can also be created by emulating (as opposed to copying directly) official servers, eg, Everquest Emulator (90). There is also a trend towards open source MMO/VW server software such as the Open Simulator Project (91).

These are examples of a trend towards open architectures. This trend may make it possible for attackers to introduce malicious servers into MMO/VWs in order to steal account information or objects of value from avatars (a sort of "virtual mugging") or disrupt game-play in other parts of the world.

3.2.13 Attacks on user's machine through game client

Like all other hosts connected to the Internet, computers taking part in games-oriented communication are prone to various network attacks. These constitute a separate category of virtual world vulnerabilities, lying in all seven layers of the OSI model (92). From an attacker's point of view, a game client is just another piece of network software that may allow them to control a user's machine. The "use" of compromised computers includes their incorporation into botnets, stealing data, and providing illegal services. The most wide-spread vulnerabilities include buffer and stack overflows, crafted network packets and the incorrect handling of parameters. The latter was discovered, for example in Second Life (93).

Clients are also vulnerable to the execution of external applications. In November 2007, a flaw in Quicktime implementation on the client allowed Second Life players to be "pick-pocketed" (94).

In this regard, there is some debate about whether the use of open source clients can open security vulnerabilities. In April 2008, an anonymous user posted the Python source code of the Eve Online client on several peer-to-peer systems. CCP, the company that released the game, claimed that it "exposes no security vulnerabilities, has no privacy protection issues, and poses no threat to our customers' billing information" (95).

It has been reported that some hybrid client and server attacks do exist. For example, after gaining control over the server, it is possible to provoke a crash of all currently connected clients by sending a crafted game message.

3.2.14 Access and authorisation problems in MMO/VWs

This class of vulnerabilities concerns the circumvention of access control restrictions to parts of the MMO/VW world.

1. **Unauthorised access to private sectors**. In worlds with private sectors authorized only to corporate employees, this can be done either by identity theft or wall-hacking (see point 3 below).

2. **Unauthorised access to data** which provides an unfair advantage. Examples include maphacking (96), and the exploitation of unintended exposures as in the *Bragg-v-Linden* case (see 3.2.4.2 "Insider **Trading"** above).

3. **Wall-hacking**. Walls in MMO/VWs visually hide content and avatars and also prevent avatars from entering certain sectors. Wall-hacking is the changing of wall properties to make them transparent to a given avatar – either disclosing information about other avatars that are hidden behind it or allowing the avatar to "walk through" it. It can also allow the use of weapons through walls.

4. **Blocking**. A group of avatars may collude to "physically" block another avatar from entering a sector of the MMO/VW space, thereby disrupting game-play.

3.2.15 Vulnerabilities in corporate worlds

3.2.15.1 Confidentiality

In corporate worlds, all documents and logs of activity are uploaded to the world at the risk and discretion of users. The issue of confidentiality is less dangerous in a private virtual world, separated from foreign networks by firewalls, but is very important in a world hosted beyond the limits of a private network. The environment is also more difficult to control than the standard means of electronic communication. Another problem is the threat of subpoena (by governments) of information disclosed within such an environment.

3.2.15.2 Difficulty of applying corporate and IT policy

Corporate security policies stipulating rules on document confidentiality and access management are much easier to enforce in the traditional environment of enterprise IT. Issues such as avatar authentication, content ownership, in-world display media and the unfamiliarity of the environment to employees can make it more difficult to enforce corporate data handling and IT policies, leading to problems such as data leakage.

3.2 15.3 Brand

Corporate presence in uncontrolled, public virtual worlds is very vulnerable to accidental or deliberate brand damage (eg, being associated with inappropriate content).

4 Recommendations and Countermeasures

In this section, we make recommendations for mitigating the risks outlined in the previous chapter.

4.1 Government Policy Recommendations

4.1.1 An industry information sharing forum for security vulnerabilities and risks

An important overall result of this report and the process of creating it has been recognition of the value of information sharing between service providers. Thus far, competitive pressures have made service providers reluctant to share information on such issues openly. There is, however, a clear need for a forum where stakeholders can share experiences of MMO/VW security issues and best practices for mitigating risk in a way which does not compromise competitive advantage, ie, sharing best practices, trends and the general characteristics of vulnerabilities without giving away corporate secrets.

Such a forum should be set up in such a way that it operates in a neutral environment and has a set of tools and procedures which foster information exchange. It should, for example, have a format for describing vulnerabilities which does not reveal sensitive information about players or corporate secrets. The members of the forum should include as many important industry stakeholders as possible and the forum should be initiated by an independent organization. Given its mandate to foster a culture of information security and bring together stakeholders in Europe, ENISA would be in a good position to stimulate such an initiative.

Such a group might also be a good forum for the definition and adoption of a common terminology to be used by providers in describing user rights and obligations. This would make it easier for users to understand what rights and risks they are dealing with.

4.1.2 Fund work on legal clarification of key issues

[Related Vulnerabilities: Avatar Identity theft and identity fraud, Risks to Intellectual property, MMO/VW Privacy Risks, Age verification, Weaknesses in Content-rating Schemes]

An important factor contributing to the impact of many vulnerabilities affecting MMO/VW assets and property (including intellectual property) is the lack of clarity in legal interpretation and in governing documents of MMO/VWs. As we have described above, the precise nature of the legal and contractual rights of end-users over virtual property is very rarely clear. Prosecutions for the theft and sale of virtual property (the underlying aim of the malware attacks) are extremely difficult and rare.

Legal clarification is an important component in addressing the increasing prevalence of cyber-attacks on virtual assets and the impact of a loss of such assets on end-users. Clarification is needed to provide a solid basis for the resolution of disputes and the prosecution of crimes committed in relation to virtual assets.

We therefore believe that work should be undertaken on the legal clarification of key issues relating to MMO/VWs. This work would not necessarily involve the information security community, although its results would have a strong impact in this area. The work should be carried out in a partnership between MMO/VW service providers and government policy makers or lawyers to produce guidelines on the interpretation of existing legislation and policy in the domain of MMO/VWs. The Council of Europe's "Guidelines to assist online games providers in their practical understanding of, and compliance with, human rights and fundamental freedoms in the Information Society, in particular with regard to Article 10 of the European Convention on Human Rights" (97) is an example of a similar set of guidelines, although it does not cover virtual worlds and some of the issues recommended below.

The key issues needing clarification are:

1. The status of original work created within MMO/VWs in relation to the underlying categories of intellectual property law. There is a need for legal clarification of the nature of the rights being created; eg, clarification of terminology, ie, whether work is copyright rather than 'IP'. EULAs should deal explicitly with IP issues, ie, whether it can be created and who owns it. In this regard, existing works such as *The Better EULA Initiative* (98) should be considered.

2. The category of copyright applicable to virtual worlds across jurisdictions, eg, literary or audio-visual work.

3. The status and rights of MMO/VW users and providers in relation to various categories of assets and contractual obligations. We emphasise that the aim is not to create new legislation, nor to apply a one-fits-all interpretation to all MMO/VW assets, but to clarify what rights apply under what circumstances.

4. The status of "acceptable risk" in relation to MMO/VWs. Sports such as boxing have a well-established body of legal precedent where organizers are able to claim exemption from certain regulations on the grounds that participants agreed to accept a certain level of risk in participating in the sport. A similar category may be appropriate in the area of MMO/VWs.

5. The definition of personal information in virtual worlds. When is data pertaining to an avatar considered as identifiable personal information about the player?

6. Further and more detailed recommendations than those provided in this paper on age-verification.

7. Many providers are subject to conflicting pressures when it comes to possible intervention in harmful content. On the one hand, there is an obligation to protect vulnerable end-users against inappropriate content (eg, minors against exposure to adult material) both from an ethical point of view and because high numbers of incidents of this nature tend to affect player numbers. On the other hand, in most legal systems intervention automatically implies that the provider gives up the right to claim "mere conduit". That is, as soon as a provider blocks or alters content, they are held responsible for it in court. Governments should investigate and if possible address MMO/VW provider concerns about conflicting obligations brought about by legislation on common-carrier status whilst at the same time ensuring that intellectual property rights are adequately protected online.

4.1.3 Financial policy

[Related Vulnerabilities: Trading and financial attacks]

The realities of selling a digital product that is consumed-on-purchase to a global market are very different from traditional e-Commerce. There is currently a serious problem in the mismatch between procedures for dealing with credit card and online payment fraud and the use-cases presented by MMO/VWs. This leads to a number of vulnerabilities in MMO/VW e-Commerce systems which create serious problems for providers and end-users. Work should be carried out by governments, in partnership with MMO/VW providers, banks, credit card companies and online payment services, to create procedures and regulations more appropriate to these environments. Such work does not necessarily involve the information security community, although it may be involved in contributing requirements.

4.2 Recommendations to Service Providers

4.2.1 Security critical implementation issues

[Related Vulnerabilities: Avatar Identity theft and identity fraud, MMO/VW specific Denial of service attacks, Attacks on user's machine through game client, Cheating, security issues]

The five most important technical issues to be highlighted in this area are:

1. **Item-duping**. Developers should be especially careful of the dangers posed by duping bugs, for example by looking very carefully at transactions across server boundaries and where multiple databases are updated simultaneously.

2. **End-to-end security** to, for example, address password and account theft. Measures should be taken wherever possible to encourage a more secure communication between the client and the server. This encompasses three

measures: authentication (both the server authenticating the client and vice-versa), integrity (making it harder for third parties or third party programs to modify data being sent), and confidentiality (encrypting sensitive server-client messages). For example, passwords should not be stored or transmitted in clear-text (and the same rule applies to all other sensitive data), rules should be applied to passwords to increase entropy, and password guessing attempts should be throttled or blocked. Where possible, the use of a second factor should be encouraged (see recommendation 4.2.4 Encourage stronger authentication). The same applies to communication between servers (eg, different "shards" of the same MMO/VW). However, as these should be on a network that is completely controlled by the operator, we expect fewer problems in securing these.

3. "The client is in the hands of the enemy", according to Raph Koster (99). Game clients should not make decisions that could affect game-play. A recent example of problems occurring as a result of not following this maxim is found in (100). Age of Conan makes the decision as to whether a player hits a target or not in the client, so that it can exactly match the timing of the animation. Since its release in May 2008, this has given rise to many bots which exploit this feature to gain unfair advantage in the game.

4. **Denial of service**. Developers should be especially careful of any game feature which gives players the opportunity to consume (or cause the consumption of) large amounts of resources such as network, processing, or world-space. Many bugs occur because players are allowed to create unlimited or self-replicating objects, or to use large amounts of processing power, etc. Developers should also be careful of any features which allow users to make external network requests since these can be used by hackers, eg, for spamming or port-scanning. Any scripting features which allow access to external resources should be limited in size and frequency and filtered for malicious content.

5. **Safeguards** should be in place against the most risky scenarios even if the risk of occurrence appears low. Most VWs use highly complex sets of rules governing behaviour and these usually become so complex that it is impossible to predict all behaviours which will emerge with large-scale use. That is, MMO/VWs are now complex enough to exhibit emergent and often highly damaging behaviours in unforeseen usage scenarios. Therefore safeguards such as bandwidth and processing limits, triggers on high transaction numbers, etc, should be built in from the start. A good approach in many cases is to whitelist allowed behaviours rather than blacklisting exceptions.

As a general comment, security in MMO/VWs should be an appropriate mix of prevention, detection and response. Many MMO/VW providers tend towards preventative measures because they provide more measureable and immediate benefits. This is often expensive and carries heavy legal responsibilities. Providers should instead create an appropriate balance between security measures aimed at detection and response and those aimed at prevention. Detection and response is often a considerably more effective (and cost-effective) means of addressing security issues in MMO/VWs.

4.2.2 Privacy policies

[Related Vulnerabilities: MMO/VW Privacy Risks]

Whilst we accept that the use and collection of data on players and avatars is often a necessary part of providing a service, this should be done in a transparent way which respects the end-user's right to informed consent. Privacy policies should therefore clearly specify:

- The types of personal (or potentially identifying) information that are collected in the context of anti-cheating measures.
- The types of personal information that are exposed to other users of the MMO/VW.
- What exactly is meant by personal data in the policy (ie, what types of data are included and excluded from its scope) and precisely what information is exposed when and to whom in the virtual world.

When specifying personal data practices, providers should take into account not only information which traditionally identifies a person such as their real name, IP address, etc, but also, following the provisions of the European Privacy Directive 95/46 and Opinion 04/2007 of The Article 29 Working Party on Data Protection on the Concept of Personal Data, any information which may reasonably used to identify a person uniquely.

4.2.3 Dispute resolution (Service Providers)

[Related Vulnerabilities: Abuse of Online Dispute Resolution]

As noted in [3.2.9], dispute resolution is very problematic in MMO/VWs due to the fact that ODR systems can be and are used to gain advantage within the game or world. Many dispute resolution systems are unworkable due to overloading by fraudulent complaints. We recommend that:

Providers should consider charging a token lodgement fee for all complaints to prevent false complaints (eg, €50). This fee could be returnable whether or not the complaint was resolved in favour of the plaintiff but would nevertheless serve to deter frivolous or fraudulent complaints.

It is interesting to note that according to the ENISA survey, a surprisingly high number of users supported the use of in-world or player-to-player dispute resolution mechanisms and courts (18).

4.2.4 Encourage stronger authentication

[Related Vulnerabilities: Avatar Identity theft and identity fraud, Problems with Online Dispute resolution, Harassment, Cheating, security issues, Information Security related Risks for Minors]

A key weak point in the chain leading from malware to identity theft and on to virtual property theft is user authentication. Several providers are now offering optional one-time password solutions; for examples, see references (11; 12). Any initiative which increases the strength of user authentication should be encouraged. Clearly this will always be an optional measure since there is usability and financial or processing cost penalties. A useful policy might be to make a second factor mandatory (or strongly encouraged using in-game or financial incentives) for the authentication of players performing any high-value or sensitive actions such as game-masters and players with access to guild bank accounts. It is interesting to note that according to the ENISA survey, 14% of users already use two factor authentication of some kind (18).

4.2.5. On governing documents

[Related Vulnerabilities: Avatar Identity theft and identity fraud, MMO/VW Privacy Risks, Problems with Online Dispute resolution, Risks to Intellectual property, Information Security related Risks for Minors]

As a way of improving governance, reducing disputes, and clarifying data protection and external security policies, we support the conclusions of Grimes, Jaeger, et al (101) whose key recommendations may be summarised as follows:

- To provide a universally accepted and standardised set of governing documents and terminology so that users can more easily find and understand them. This work would have to be carried out as a collaborative effort between providers.
- To provide a single point of reference where governing documents may be obtained.
- To encourage input from and the participation of end-user groups in the design and development of governing documents.

4.2.6 Live CDs as a more secure option

[Related Vulnerabilities: Avatar Identity theft and identity fraud, Attacks on user's machine through game client]

Live CDs and DVDs are a well-known measure to improve security in critical online operations such as online banking. A live CD is a complete operating system on a CD, which requires no installation and no files stored on the PC hard drive (although session data may be written). It can improve security because it prevents malware from accessing operating system files and separates the operating system used in critical operations from that used in day-to-day browsing where malware vectors are more common.

Such as solution could also be an *option* for MMO/VW providers. They could provide a bootable CD image for download which contains an operating system with the game ready installed. This is certainly not a solution which could be universally applied or made obligatory, since it adds considerable time and inconvenience to the user experience. However, as with stronger authentication, it is something which could be offered to the more security-conscious user and which might improve the overall security of the user-base. We note that the operating system would have to be freeware (eg, Linux) since it would otherwise be too expensive, and that this option only applies to certain games or worlds and not, for example, to those operating in a browser.

4.3 Awareness-raising and research

Awareness raising is a very important countermeasure to many of the threats outlined above. More information on how to conduct awareness raising campaigns can be found in reference (102). In general, it is important to use in-context methods to raise awareness. For example, when logging in, a link could be provided to a video about how to detect account compromise, or about the advantages of stronger authentication methods. When creating in-world content, a link could be provided to a user-friendly explanation of the user's IP rights.

This section describes the issues we consider the most important and which should be highlighted in any awareness raising campaign.

4.3.1 Detection of account compromise

[Related Vulnerabilities: Avatar Identity theft and identity fraud]

Given the increasing prevalence of identity theft in virtual worlds, it is important to raise users' awareness of how to detect account compromise. The following is a check-list which could be used:

- Your character is not in the same place as when you logged out.
- Some of your items are missing.
- Your password is incorrect.
- There are new people on your friends list.
- Some of your characters are missing, or there are new characters.
- The last login on the Account Management does not match when you last logged on.
- You have received an e-mail from the Game Masters with a warning for something that happened when you were not online.
- Your guild members say that they have seen your character online when you were not playing.

4.3.2 Age verification and risks to minors

[Related Vulnerabilities: Information Security related Risks for Minors]

ENISA's paper, "Children on virtual worlds, What parents should know" (103), gives 25 detailed safety tips (recommendations) specifically aimed at improving safety for minors by giving advice to parents. In this section, we therefore only address some specific points which this group considers particularly important in this area.

- All users should be made aware that age verification mechanisms currently have a low success rate and therefore they should not place too much faith in the claimed age of other users.
- Minors should be educated on how to detect and respond to inappropriate behaviour by adults who have infiltrated games designed for minors. The following is a suggested check-list:
    - Never give away your physical contact details even to an avatar.
    - Never agree to meet anyone you have met in a MMO/VW in person, especially without consulting an adult first.
    - Do not respond to inappropriate (ie, bullying, obscene or offensive) messages via chat and report them to an adult.
    - Never give away your account password or username.
    - Be especially careful with your virtual possessions and money or coins, and beware of anyone asking you to give them away for any reason.
    - Be aware that other players may give false information about real-world characteristics.
- Minors should be made aware of the most important risks posed by playing games designed for adults only (such as physical meetings, sexual content, and loss of real money). This does not mean that they should be encouraged to play them. However, given the large numbers of minors who do play such games, we believe they would be less vulnerable if they were better informed of the risks.
- Children should be made aware of the risks and ethical consequences of viewing or posting illegal copyrighted content within games.
- Parents and teachers should be made aware of all the above risks in order to better protect their children. This information should be transmitted through multiple media channels since many parents do not play online games.
- Parents should be made aware of the risks of relying on age-verification mechanisms to protect children and the need for non-automated monitoring of game usage.
- Parents should be made aware of the risks of relying on content filtering tools. Studies, such as (104), show that content filtering is far from reliable, particularly in the area of online games.

4.3.3 Data Privacy

[Related Vulnerabilities: MMO/VW Privacy Risks]

The use and collection of in-game data plays an increasingly important role in the economic models of most providers. Whilst this is in many cases necessary to maintain service, users should nevertheless be made aware of the possible privacy threats from playing online games. In particular:

- The use of an avatar is not necessarily a protection against the disclosure and collection of sensitive personal information.
- Sensitive data, such as chat messages, may be eavesdropped by other characters or even in-world objects.
- Actions carried out in-world may be linked to a real-world address by the service-provider, sometimes even when false registration information is given.

4.3.4 In-world property

[Related Vulnerabilities: All (most attacks aim to steal virtual property)]

Users should be made more aware of the risks to their in-world property. In particular:

- If the provider may permanently delete or confiscate assets without warning, users should be aware of this fact and take it into account when valuing the assets. According to the ENISA survey, only 41% of users were aware of this as a possibility (18).
- The risk of theft due to account compromise and the options open to them should this happen.
- Other risks to property such as devaluation due to duping, induced character suicide, etc.

4.3.5 In-world Intellectual Property

[Related Vulnerabilities: Risks to Intellectual property]

Some MMO/VWs give users the right to intellectual property over creations in-world. Specification of the exact nature of such rights is however extremely vague. Users should be informed of the exact rights they have to in-world creations, in particular:

1. Whether components (eg, textures) of the creation are subject to subsidiary rights;
2. The types of work covered by IP rights (eg, whether objects created using in-world tools, arrangements of objects, etc, are covered);
3. The dangers of posting or incorporating other copyrighted work;

4. What options the user has if their rights are infringed; and

5. The IP laws that apply, ie, the jurisdiction, eg, the US, UK, etc.

4.3.6 Corporate Virtual Worlds

There is very little research on the security of corporate virtual worlds, even though this is an emerging technology with a big potential to develop in the course of the next few years. We therefore recommend that enterprise-critical data should not be processed within a virtual world that is not entirely under the company's control and that no client or server beyond a protected local area network, administrated by trusted parties, should be used. Special attention should be given to authentication methods and the enforcement of corporate IT policies within such environments.

4.3.7 Research directions

[Related Vulnerabilities: All]

We recommend that the following should be the subject of scientific research funded by the European Commission:

- The security and reliability issues of open world formats. The trend towards open MMO/VW formats for clients and servers has important implications for security, reliability and privacy. Research should be undertaken, for example, into:
    - Security and scalability of transaction management and simultaneity in open worlds;
    - Protection against malicious servers (avatar mugging); and
    - Open world data protection policies which can be applied across multiple servers/providers.
- Privacy, identity and anonymity in virtual worlds, including measures against real-world profiling in virtual worlds.
- Security issues of virtual world economies.
- Effective content filtering for MMO/VWs.
- Effective age verification for MMO/VWs.
- Security vulnerabilities in corporate worlds, including how to ensure the confidentiality and integrity of data processed within virtual worlds, how to facilitate administrative control and the enforcement of security policies, and how to enhance identity and access management.

5 Appendix I Classes of MMO/VWs and their security-relevant features

The following tables show how the above security relevant features are implemented in different classes of MMO/VWs. An example from each class has been taken to illustrate the implementation of security relevant features [2].

5.1 Civic Worlds – Second Life

Feature	**Civic (Second Life)**
EULA	Second life is governed by *Second Life EULA* (105). Interesting features from a security and vulnerability point of view include: • You must be over 18 to play • You should not lie about your personal information • Transfers of accounts to other people are not permitted • No impersonation is allowed • Land use is paid in arrears • Any data residing on Linden's servers may be reset at any time for any or no reason • Linden does not recognise cash value for items • Linden Dollars represent a limited license right governed solely by the terms of the end-user license agreement • No spamming is allowed in–world • No denial of service attacks are allowed • Identity theft is forbidden • Stalking or harassment is forbidden • Users may have IP rights to content
Player-to-player governance	Some courts and in-world lawyers, private zones
Scripting features	• Users may create scripts attached to objects within the world • Scripts can access outside network resources • Scripts can be activated by other users • Some interesting scripting functions from a security point of view:

	• XML RPC • LlGetLandOwnerAt • LlRequestAgentData • HTTP Requests • PERMISSION_ATTACH
Trading possibilities	• Objects, services and land may be bought and sold in exchange for Linden Dollars • Sale outside of SL is forbidden
AVATAR Actions and value-transfer possibilities	• Instant messaging using SL client • Voice over IP • Pushing and "physical" signs
Client features	• Open source • No world data stored on the client machine
Server features	• Open protocol • Data is stored on Linden servers according to geographical areas, called SIMs, each run by a single server.
Automation possibilities	• Fully automatable • No rules against this - no bot detection
Player tracking and behaviour analysis	Eavesdropping in local vicinity is possible
World culture	The main objective is to create social capital. A secondary objective is in-game wealth.
User content creation	• Users may create buildings, scripted objects • Users may own IP
Identity policies/culture	• Link to real-world identities • Impersonation is discouraged • Persistence of identity is encouraged
Dispute resolution	Incident reports handled by Second Life Governance Team
Financial System	Linden Dollars can be bought for real money. Linden Dollars represent a limited license right governed solely under the terms of the EULA.
Access control	• Username password (stored as hash with MAC address on user's machine) • Physical blocking possible • Private areas possible

5.2 Gaming/Ludic Worlds – World of Warcraft

Feature	Game (World of Warcraft)
EULA	Governed by EULA (106) and Terms of Use (107). Interesting features from a security and vulnerability point of view include: • You must be an adult in your country • You may not share account and login information with anyone (excluding one minor of whom you are a parent or guardian) • "All rights and title in and to the Program and the Service are owned by Blizzard or its licensors" • No selling, leasing or licensing of the Game to others • No hacking, cheating, or modification of content
Player-to-player governance	Guilds
Scripting features	Macros – see (108)
Trading possibilities	• Trading in-game, using game currency to be used only in the world • Trading any part of game content outside the game for real money is forbidden
AVATAR Actions and value-transfer possibilities	• Built-in mail system • Chat channels • Emoticons • Voice chat
Client features	Commercial only
Server features	• User Interface information, settings, key-bindings, add-ons stored on local machine • Some of the user settings stored on servers • World data stored on Blizzard servers • Different game servers for different geographical locations • Dedicated servers for various game areas, eg, instances, battlegrounds, different continents
Automation possibilities	• Macros allowed to some extent • Automation of the game is not allowed • Bot detection program Warden

Player tracking and behaviour analysis	Avatar information/history can be recorded and published – see for example reference (109)
World culture	Fantasy/Game – objective is to explore the world, complete quests and bring characters to higher levels.
User content creation	• No user game-content creation • Creation of Machinima movies using products copyrighted by Blizzard • Fan art – screensavers, wallpapers • Capturing screens
Identity policies/culture	• Giving your character a name that corresponds with a real life name is against Naming Policy • No obvious link between game character and real life person
Dispute resolution	• Ticketing system – player who feels abused, harassed, or wants to complain about other players behaviour can report such players via reporting system • Game Masters (GM) contact players to solve the problem • Claims regarding content loss, login information theft, account problems should be reported through email, ticket, web form or telephone
Financial System	• Game currency – Gold • World economy is similar to a real world economy – the same rules apply as in real life (eg, supply, demand) so it is very susceptible to unauthorised gold, duping of objects, monopoly, etc • Each server has its own independent economy • Servers behave like countries – young servers have economies similar to developing countries
Access control	WoW Authenticator (2 factor OTP based) available

5.3 Social Worlds – Habbo Hotel

Feature	Social (Habbo)
EULA	Governed by *Habbo EULA* (110) EULA (or Terms of Service) may vary depending of the region and the country, though the basics of the EULAs remain the same. Some Important features : • The age limit varies depending on the country – for example, in Finland the age limit is 10 and in the US it is 13 • Site or content created may not be used for commercial purposes • Habbo accounts that are old, unused or passive for six months or more, will be deleted without notification on a regular basis • No spamming • Defamation, abuse, harassment, stalking, threatening or otherwise violating the legal rights (such as rights of privacy and publicity) of others are forbidden • Publishing, posting, uploading, distributing or disseminating any inappropriate, profane, defamatory, infringing, obscene, indecent or unlawful topic, name, material or information is forbidden. • To advertise or offer to sell or buy any goods or services for any business purpose is forbidden • Harvesting or otherwise collecting Personal Data (as defined below) about others, including email addresses, is denied • Creating a false identity, or impersonating any person or entity, for the purpose of misleading others is forbidden • Forging headers or otherwise manipulate identifiers in order to disguise the origin of any material transmitted through the Service is forbidden • No furniture or Habbo coin theft • All purchases of Habbo coins and/or of premium subscriptions and/or of any other virtual items (eg, furniture) sold on the site are final and non-refundable, except at the sole and absolute discretion of the service provider, and are a limited game play license and not a cash account or equivalent. Once you buy coins, a premium subscription or any other virtual item sold on the site, you cannot get your money back.

Player-to-player governance	• Private rooms, kicking and banning from room, "invite only" rooms, muting a player • Calls for help
Scripting features	None
Trading possibilities	• Objects may be bought and sold in exchange for Habbo coins • Sales outside Habbo are forbidden (111)
AVATAR Actions and value-transfer possibilities	• Instant messaging using Habbo client • Habbo mail • Message boards • Habbo homepages
Client features	• Shockwave based • Does not store data on client computer
Server features	• Game data is stored in Habbo Hotel servers which are managed by Sulake Corporation. Game data available in one Habbo Hotel instance is not available in others. • Client server traffic is encrypted
Automation possibilities	None
Player tracking and behaviour analysis	• All time moderated, some moderation automated
World culture	Primarily a social meeting place for teenagers; see *Habbo Culture* (112)
User content creation	Active user content creation
Identity policies/culture	• No direct link to real-world identities • Impersonation is discouraged
Dispute resolution	Reports can be made through Habbo Help Tool
Financial System	Habbo-coins can be purchased for real money. Habbo coins are used to buy goods in the game. See *Habbo Credits* (113)
Access control	• Habbo-account, password and account name • Account confirmation via a valid email address • CAPTCHA used in certain circumstances to prevent brute forcing and computer based automations • To recover lost password, need to have access to defined email and need to know date of birth

5.4 Corporate Worlds - Qwaq

Feature	Corporate (Qwaq)
EULA	Governed by EULA presented upon installing software. Interesting features: • Users agree to be the sole parties responsible for the content and not to use the service in an irregular way (spam, harassment, copyright infringement, etc) • Use is only for internal business purposes • Reverse engineering is forbidden • All uploaded or downloaded data are at risk and discretion of the user
Player-to-player governance	Corporate rules
Scripting features	• No direct scripting possible
Trading possibilities	None
AVATAR Actions and value-transfer possibilities	• Built-in VoIP • Text chat
Client features	• Microsoft Windows XP, Mac OS X (Linux under development) • All communication between users is automatically encrypted
Server features	• Peer-to-peer architecture • Qwaq Forums is built on an open model for developing and delivering deeply collaborative multi-user online applications. Qwaq Forums also uses the Python programming language for scripting and standard XML interfaces for application integration. • For customers who want to deploy Qwaq Forums behind corporate firewalls, Qwaq will deliver the server as an appliance for deployment behind their firewall.

Automation possibilities	None
Player tracking and behaviour analysis	• Logging possible
Game culture	• Users can occupy many different Qwaq forums as appropriate, allowing them to work on different topics with different teams. • Different users can have different levels of access to Qwaq forums; for example, employees might have access to spaces that business partners do not. • Qwaq Multi-Share allows users in the same virtual space to see how others are editing or modifying content. It allows multiple users to quickly and intuitively share control of an application or content.
User content creation	• Pre-built templates for different types of spaces • Most content can be added using drag-and-drop placement.
Identity policies/culture	Real-world and corporate identity is most usual.
Dispute resolution	• N/A – business environment
Financial System	• N/A – business environment
Access control	• To access any workspaces, users or companies must be explicitly invited. • Users need to authenticate to join a virtual space. User credentials can be checked against an existing authentication service such as Active Directory or LDAP in the self-hosted edition.

6 References and Links

All web resources verified in November 2008.

1. **Bartle, Richard.** *Designing Virtual Worlds.* s.l. : New Riders, 2003.

2. **Reynolds, Ren.** The Four Worlds Theory. 08 2005. http://terranova.blogs.com/terra_nova/2005/08/the_four_worlds.html.

3. Gaming and Virtual Worlds Survey Results. http://www.enisa.europa.eu/doc/pdf/deliverables/VW_Survey.pdf.

4. Kaspersky online gaming 2007. http://www.viruslist.com/en/analysis?pubid=204791985.

5. **Seiler, Joey.** More Cyber Thieves Prefer Virtual Money to Real. 06 2007. http://www.virtualworldsnews.com/2007/06/more-cyber-thie.html.

6. **Lehtiniemi, Tuukka.** How big is the RMT (Real Money Trading) market anyway? 03 2007. http://www.virtual-economy.org/blog/how_big_rmt_market_anyway.

7. Entropia Universe home page (claim of 360 Million US$ turnover). http://www.entropiauniverse.com.

8. Mindark Annual Report. 2007. ftp://ftp.mindark.se/reports/AnnualReport2007_LOW.pdf.

9. World of Warcraft Europe. http://www.wow-europe.com/en/index.xml.

10. World of Warcraft reaches 10 million users worldwide. 2008. http://www.blizzard.com/us/press/080122.html.

11. Blizzard Authenticator offers enhanced security for World of Warcraft accounts. http://www.blizzard.com/us/press/080626-auth.html.

12. Entropia Gold Card security system. http://www.entropiauniverse.com/en/rich/6399.html.

13. Alley Insider - Habbo Facts. 2008. http://www.alleyinsider.com/companies/habbo.

14. Habbo hotel figures. 09 2008. [Cited: 22 09 2008.] http://www.sulake.com/habbo/.

15. GameUSD.com. 2008. http://www.gameusd.com/.

16. eBay Online Auction Site. http://www.ebay.com.

17. **Heeks, Richard.** Current Analysis and Future Research Agenda on Gold Farming. http://www.sed.manchester.ac.uk/idpm/research/publications/wp/di/documents/di_wp32.pdf.

18. **ENISA.** Reputation-based systems:a security analysis. http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_reputation_based_system.pdf.

19. **Yee, Nicholas.** Everquest survey - 889 Users polled. 2001. http://www.nickyee.com/eqt/report.html.

20. OpenSimulator. http://opensimulator.org/wiki/Main_Page.

21. IBM Linden Labs interoperability announcement. http://blog.secondlife.com/2008/07/08/ibm-linden-lab-interoperability-announcement/.

22. OpenSimulator project. http://opensimulator.org/wiki/Main_Page.

23. Web 3D: The Next Major Internet Wave. http://www.forrester.com/Research/Document/Excerpt/0,7211,45257,00.html.

24. Web 2.0 to Web 3D. http://reality.org/2007/03/13/sxsw-panel-web-20-to-web-3d-part-1/.

25. IGE MMORPG Services. http://www.ige.com/.

26. Here Come da Judges: Second Life Superior Court is Now in Session. http://www.secondlifeherald.com/slh/2005/09/here_come_da_ju.html.

27. Portuguese Ministry of Justice to Open Alternative Dispute Resolution Facility in Second Life. 07 2007. http://virtuallyblind.com/2007/07/27/portuguese-ministry-justice-adr-second-life/.

28. Council of Stellar Management. http://myeve.eve-online.com/download/devblog/CSMSummary.pdf.

29. Linden Scripting Language. http://wiki.secondlife.com/wiki/LSL_Portal.

30. Request Agent Data (Second Life Scripting function). http://wiki.secondlife.com/wiki/LlRequestAgentData.

31. Club Penguin. http://www.clubpenguin.com.

32. **Biancuzzi, Federico.** Real Flaws in Virtual Worlds - State Management Flaws. *Security Focus.* 12 2007. http://www.securityfocus.com/columnists/461/2.

33. Pan European Game Information System. http://www.pegi.info/.

34. Entertainment Software Ratings Board. http://www.esrb.org/ratings/ratings_guide.jsp.

35. **PEGI.** *NICAM Activity Report – July 2008.*

36. Mass bannings strike Glider users. 05 2008. http://nihilum.mousesports.com/en/news/693,banwave_on_people_using_glider/.

37. World of Warcraft 2.3 updates Warden - Botters Complain. http://www.yougamers.com/news/14407_world_of_warcraft_2_3_updates_warden_-_botters_complain/.

38. Gartner Press Release. 05 2008. http://www.gartner.com/it/page.jsp?id=670507.

39. **Dignan, Larry.** IBM cooks up internal virtual world for confidentiality, security. 12 2007. http://blogs.zdnet.com/BTL/?p=7382.

40. **Network, Virtual Economy Research.** How big is the RMT market anyway? 03 2007. http://www.virtual-economy.org/blog/how_big_rmt_market_anyway.

41. **Strategy Analystics.** Online Games: Global Market Forecast. 08 2007. http://www.strategyanalytics.com/default.aspx?mod=ReportAbstractViewer&a0=3559.

42. *'Machinima and Copyright Law.* **Freedman, Matthew Brett.** 235, 2005, Vol. Journal of Intellectual Property.

43. *'Fostering Creativity in Virtual Worlds:Easing the Restrictiveness of Copyright for User-Created Content.* **Todd, David Marcus.** 52, 2008, Vol. New York Law School Law Review. 67.

44. BODY DOUBLES SHAPES~Most Celebrity Shapes* in SL! http://world.secondlife.com/place/1dd53ee7-35fb-6a0d-6866-1b3177211705.

45. IFrame malware vectors - sophos security analysis - top malware vector December 2007. http://www.sophos.com/security/analyses/viruses-and-spyware/maliframef.html.

46. Sophos IFrame Worm No 1 in December. 04 01 2008. http://www.darkreading.com/document.asp?doc_id=142350.

47. *A Study of Malware in Peer to Peer.* **Andrew Kalafut, Abhinav Acharya, Minaxi Gupta.** Rio de Janeiro : s.n., 2006. Proceedings of the 6th ACM SIGCOMM conference on Internet measurement. pp. 327 - 332. http://portal.acm.org/ft_gateway.cfm?id=1177124&type=pdf&coll=GUIDE&dl=GUIDE&CFID=2023596&CFTOKEN=52802835.

48. Infostealer.Wowcraft.D Symantec Description. http://www.symantec.com/security_response/writeup.jsp?docid=2006-061911-0328-99.

49. Wowui.incgamers.com invaded by malware. 4 2008. http://www.wowinsider.com/2008/04/14/wowui-incgamers-com-invaded-by-malware/.

50. WoW Ace Updater ad banners may contain Trojans, claim some users. 04 2008. http://www.wowinsider.com/2008/04/16/wow-ace-updater-ad-banners-may-contain-trojans-claim-some-users/.

51. Information For Consumers - Protecting Your Identity In The Virtual World. 2003. http://www.bbbonline.org/IDTheft/virtual.asp.

52. Trojan targets World of Warcraft gamers. 05 2006. http://www.theregister.co.uk/2006/05/08/wowcraft/.

53. **Leyden, John.** Trojan targets World of Warcraft gamers. 05 2006. http://www.theregister.co.uk/2006/05/08/wowcraft/.

54. **Clive Thompson.** Identity theft: The ultimate role-playing game. 08 2005. http://www.collisiondetection.net/mt/archives/2005/08/antivirus_compa.html.

55. Warcraft gamers locked out after Trojan attack. 12 2006. http://www.theregister.co.uk/2006/09/29/warcraft_trojan_attack/.

56. What is a compromised account? (World of Warcraft). http://www.wow-europe.com/en/support/ca-article.html.

57. When World of Warcraft spreads to your world, How enterprise networks can take collateral damage. http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9016684.

58. **Koster, Raph.** A Declaration of the Rights of Avatars. 08 2000. http://www.raphkoster.com/gaming/playerrights.shtml.

59. European Privacy Directive 95/46. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

60. On WoW Warden. 11 2007. http://onwarden.blogspot.com/2007/11/storm-is-brewing.html.

61. ContextAds behavioural marketing tool based on in-game eavesdropping. http://www.slcontextads.co.uk/about.asp.

62. PC/Web Games Ad Revenue (including Virtual Worlds) to reach $152 Mill by 2011. *Virtual Worlds News.* 07 2007. http://www.virtualworldsnews.com/2007/07/pcweb-games-to-.html.

63. Thottbot - service with information about other players in World of Warcraft. http://thottbot.com/.

64. **Castronova, Edward.** Effects of Botting on World of Warcraft. http://virtuallyblind.com/files/mdy/blizzard_msj_exhibit_7.pdf.

65. Thottbot collects information about other users in World of Warcraft. http://thottbot.com/.

66. WoW Warden - wikipedia. http://en.wikipedia.org/wiki/Warden_(software).

67. On Warden's use of polymorphism. 11 2007. http://onwarden.blogspot.com/2007/11/storm-is-brewing.html.

68. Hernandez v IGE. http://virtuallyblind.com/2007/12/11/ige-will-answer-complaint/.

69. The9 Loses Gold Farming Suit To WoW Gamer. http://www.pacificepoch.com/newsstories?id=129797_0_5_0_M.

70. *Online Games and Security.* **Gary McGraw, Greg Hoglund.** 5, Privacy and Security, Vol. 5, pp. 76-79. http://www.cigital.com/papers/download/attack-trends-EOG.pdf.

71. Race conditions - definition. http://en.wikipedia.org/wiki/Race_condition.

72. **Terdiman, Daniel.** Cheaters slam 'Everquest II' economy. 08 2005. http://news.zdnet.com/2100-1040_22-144176.html.

73. The In-game Economics of Ultima Online. 1999. Chapter 5. http://www.mine-control.com/zack/uoecon/uoecon.html.

74. Asheron's Call Dupe Bug. 09 2004. http://www.taultunleashed.com/phpbb2/post-174400.html.

75. World of Warcraft Duping Bug. http://www.edgeofnowhere.cc/viewtopic.php?t=300253&sid=1485f9d8d5b68c50b3c6c279b5cb9de9.

76. Bragg vs Linden case. 06 2007. http://forge.ironrealms.com/2007/06/29/bragg-vs-linden-linden-strikes-back/.

77. Explanation of Kill Stealing. 07 2004. http://wowvault.ign.com/View.php?view=Totw.Detail&id=29.

78. Summary of the Blizzard vs Glider case. http://virtuallyblind.com/category/active-lawsuits/mdy-v-blizzard/.

79. Second Life Copybot. http://en.wikipedia.org/wiki/CopyBot.

80. Digital Millenium Copyright Act. *Library of Congress.* 1998. http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281:.

81. Marvel v NCSoft, Memorandum of Points and Authorities of Amici Curiae,. 21 October 2005. http://www.eff.org/files/filenode/Marvel_v_NCSoft/NC-MemPointsFinal.pdf.

82. Linden Labs Blog - Abuse Reporting Begins Overhaul. 12 2006. http://blog.secondlife.com/2006/12/08/abuse-reporting-begins-overhaul/.

83. Second Life Peak User Statistics 2006-2008. http://secondlife.com/whatis/economy-graphs.php.

84. DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the processing of personal data and the protection of privacy in the electronic communications sector. 2002. http://eur-lex.europa.eu/pri/en/oj/dat/2002/l_201/l_2012002.

85. DDoS Attacks Target Final Fantasy XI. 04 2005. http://news.netcraft.com/archives/2005/04/19/ddos_attacks_target_final_fantasy_xi.html.

86. **Miller, Richard.** Malware Knocks Virtual World Offline (Second Life attacked by instant messaging bot). 11 2005. http://news.netcraft.com/archives/2005/11/14/malware_knocks_virtual_world_offline.html.

87. Widespread Outages for World of Warcraft. http://news.netcraft.com/archives/2006/03/25/widespread_outages_for_world_of_warcraft.html.

88. 'Second Life' fending off denial-of-service attacks. 05 2006. http://news.cnet.com/Second-Life-fending-off-denial-of-service-attacks/2100-1043_3-6067003.html.

89. Youtube video - Dark Age of Camelot Blocking DOS. 06 2008. http://pl.youtube.com/watch?v=s-rl3RPC_Mw.

90. Everquest Emulator. http://www.eqemulator.net/main.php.

91. Open Simulator Project. http://opensimulator.org/wiki/Main_Page.

92. List of game vulnerabilities. http://securityvulns.com/news3478.html.

93. Second Life URI Handler Registration Vulnerability. http://secunia.com/advisories/26845.

94. Second Life Viewer Susceptible to Quicktime Security Flaw. http://blog.secondlife.com/2007/11/30/second-life-viewer-susceptible-to-quicktime-security-flaw/.

95. Eve online source code leaked. 04 2008. http://www.gamesindustry.biz/articles/ccp-plays-down-eve-online-source-code-leak.

96. Maphacking - definition. http://en.wikipedia.org/wiki/Maphack.

97. Protecting human rights on the Internet - Council of Europe launches guidelines in cooperation with online games and Internet service providers . http://www.isfe.eu/index.php?PHPSESSID=t7cjd5ja7gtvie9454k9tocij1&oidit=T001:96dec7f314175b346499b34f5ad64fda.

98. The Better EULA Initiative. http://www.bettereula.com/index.php?title=Main_Page.

99. **Raph Koster.** *The Laws of online world design.* http://www.raphkoster.com/gaming/laws.shtml.

100. Example of Bots written for Age of Conan. http://www.msxsecurity.com/ageofconanhacks.php.

101. **Grimes, J. Jaeger, P Fleischmann, K.** Obfuscatocracy: a stakeholder analysis of governing documents for virtual worlds. FirstMonday: Peer-reviewed Journal on the Internet, 09 2008.

102. **ENISA.** The new users' guide: How to raise information security awareness. http://www.enisa.europa.eu/doc/pdf/deliverables/new_ar_users_guide.pdf.

103. **ENISA.** Children on virtual worlds, What parents should know. http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf.

104. **Safer Internet Plus Programme / Deliotte.** Safer Internet - Protecting Children on the Net: Test and benchmark of products and services to filter Internet content for children between 6 and 16 years. http://www.sip-bench.eu/Reports2007/SIP%20Bench%202007%20-%20Synthesis%20Report.pdf.

105. Second Life EULA. http://secondlife.com/corporate/tos.php.

106. World of Warcraft EULA. http://www.worldofwarcraft.com/legal/eula.html.

107. World of Warcraft Terms of Use. 11 2007. http://www.worldofwarcraft.com/legal/termsofuse.html.

108. World of Warcraft Macros. http://www.worldofwarcraft.com/info/basics/macroguide-one.html.

109. Avatar history available here for World of Warcraft. http://www.warcraftrealms.com/charhistory.php.

110. Habbo EULA. 06 2008. http://www.habbo.com/papers/termsAndConditions.

111. Habbo Trading Help. http://www.habbo.com/help/63.

112. Habbo Culture. http://www.sulake.com/habbo/?navi=2.

113. Habbo Credits. http://www.habbo.com/credits.


enisa
European Network
and Information
Security Agency

PO Box 1309, 71001 Heraklion, Greece, Tel: +30 2810 391 280
www.enisa.europa.eu