Journal of
Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Volume 3, Number 3
The Researcher's Toolbox, Part II
May 2011

Editor-in-Chief Jeremiah Spence

Image Art ©2007-2011 ~enchanted-stock
http://fav.me/dwquz0

Technical Staff John Brengle
Betsy Campbell
Sil Emerson

Journal of Virtual Worlds Research
jvwresearch.org ISSN: 1941-8477

Volume 3, Number 3
The Researcher's Toolbox, Part II
May 2011

Massively Multi-Player Online Role Playing Games: What's the Risk?

Benjamin Sanders
University of Plymouth, United Kingdom

Paul Dowland
University of Plymouth, United Kingdom

Shirley Atkinson
University of Plymouth, United Kingdom

Steven Furnell
University of Plymouth, United Kingdom

Abstract

Some may argue that the proliferation of personal computers together with the widespread use of the Internet has brought many benefits to society. The popularity of the internet and its associated online services continues to grow at an exponential rate and consequently, so does the number of avenues for potential exploitation. Prior research has already established that sexual predators and social engineers use the Internet as a means to target and exploit individuals. Indeed, previous studies highlight the significant threats faced by users of instant messaging and social networking facilities. Online role-playing games and virtual environments provide yet another platform for users to interact with one another. Evidence suggests that subscribers of such services often become so immersed in a fantasy world that their ability to differentiate between the virtual and real world is reduced. This monograph investigates the level of threat faced by users of virtual environments and online role-playing games. The study made use of an online survey to assess the current level of awareness and understanding amongst individuals who spend excessive amounts of time engaging in such environments.

Keywords: MMORPG; Massively Multi-Player Online Role Playing Games; 3D; risk

Massively Multi-Player Online Role Playing Games: What's the Risk?

In recent years we have witnessed the rapid development and global embrace of Massively Multi-Player Online Role Playing Games (MMORPGs). MMORPGs provide subscribers with a graphically rich, fully immersive 3D fantasy world in which like-minded individuals can interact and collaborate to accomplish complex and challenging tasks. For some, however, these engrossing worlds have become an alternative lifestyle which takes precedence over reality (Öqvist, K.L., 2009).

Online privacy and social engineering are subjects of extensive research, and it is commonly acknowledged that the internet is embraced by individuals with darker motives. Awareness raising campaigns provide children with valuable information on how to protect themselves online, however, studies reveal that a lack of awareness amongst young online gamers could lead to negative consequences (Microsoft, 2010). Evidence suggests that MMORPG environments are becoming an emerging avenue for exploitation, yet millions of subscribers are divulging personal and sensitive data to fellow gamers with whom they have built, what they perceive to be, close relationships. In reality, however, many such relationships are formed with complete strangers and can lead to dangerous consequences with victims falling foul to attacks of grooming and social engineering to name but two (Gladwell, 2009).

The design of MMORPG environments not only forces participants to collaborate with complete strangers but also entices end-users to play continuously for an excessive number of hours. Evidence suggests that the addictiveness of such environments is not only damaging to mental health and general well-being, but is also leaving individuals vulnerable to exploitation. A recent study at the University of Plymouth investigated this issue with 362 online gamers; gamers were asked about their gaming habits and in-game security awareness (Sanders, Furnell, Dowland, 2009).

The study revealed that almost a quarter (23%) were classified as addicted to online gaming, with many players experiencing negative lifestyle changes as a result of their engagement with MMORPG's. The study collated the following evidence highlighting addictive tendencies:

- 29% attempted to cut down the amount of time spent playing MMORPG's but were unsuccessful.
- 63% found themselves spending increasing amounts of time online.
- 85% frequently found themselves staying up until late into the evening playing MMORPG's.
- 80% often found themselves thinking about the game when they were not physically playing

Such findings highlight the addictive nature of online gaming. Unfortunately the dangers associated with MMORPGs do not solely rest with excessive use. The study revealed that 80% of participants had formed particularly close friendships with fellow gamers whist 96% openly discussed personal issues not related to game play. The affordances of anonymity can create hyper-personal interaction between online participants, invoking more self-expression and idealised self-presentation. However, the combination of addiction intertwined with such hyper-interaction creates an emerging avenue for exploitation.

Indeed, the aforementioned statements correlated with further findings from the authors' study:

- 89% had previously divulged personal and sensitive data in an MMORPG environment, including age (81%), location (77%), and email addresses (48%).
- 38% sent personal pictures to online friends upon request.
- 22% previously divulged personal telephone numbers.
- 10% had divulged MMORPG account credentials upon request

In a previous study at the University of Plymouth, 86 respondents were surveyed about their security awareness within social networking environments. A comparison of both studies found that social networking users showed a greater level of awareness regarding the disclosure of personal and sensitive data within online interactive environments compared to MMORPG subscribers. Indeed, 61% of social networking participants disclosed their age compared with 81% of MMORPG subscribers, 10% their location compared to 77% and 52% their email addresses compared to 48%. (Sanders, Dowland, Furnell, 2009). The findings indicate that both

respondent groups share the same view of divulging email addresses but the respondent group's view of location differed significantly. The authors theorise that this is due to social networking being more closely linked to real-life, making users more aware of the dangers. In addition, Yee (2003) notes that MMORPG environments encourage idealisation of the self and the chivalric romance embraced in such environments can potentially create a false sense of trust amongst players. Consequently this provides a heightened opportunity for predation and exploitation.

In addition, almost half (45%) of respondents had become suspicious of other players' behaviour whilst engaging with MMORPGs. Respondents reported concerns including: stalking, harassment, racism, stealing of online currency and property, and extreme aggressive behaviour. Further case studies at the University of Plymouth revealed that of the 23% who were classified as behaviourally addicted to MMORPGs, 16% have been subject to social engineering attacks, of which 5% fell victim to successful attacks including fraud and being duped into sending sexually explicit pictures.

In a more recent study, the authors undertook an identical body of work in Greece, supported by the University of the Aegean. 100 respondents were surveyed on their security awareness within MMORPG environments. The results between the two studies proved to be very similar. Indeed, 82% of Greek MMORPG subscribers disclosed their age compared with 81% of English subscribers and 64% their location in contrast to 77%. In addition, 61% revealed their real name and 45% their interests. Moreover, 42% of Greek MMORPG subscribers disclosed their email addresses compared to 48% from the previous study, 27% their personal pictures compared to 38%, 22% their personal telephone numbers in contrast to 21%. The results give a clear indication that the majority of MMORPG subscribers consider their virtual data to be of greater importance than their personal data. However, previous studies highlight the potential dangers associated with the aggregation of personal and sensitive data.

The findings present clear evidence that security awareness amongst online gamers is an area for concern and further research. Moreover, there are few technological frameworks implemented within MMORPG infrastructures that protect the online gamer, therefore creating the need for awareness raising to cultivate an effective security culture amongst the gaming population. To achieve the aforementioned aims, continued efforts to educate the end-user must be applied to increase understanding and minimise the risks inherent with MMORPG engagement.

This places an onus on MMORPG vendors to provide appropriate safeguards and awareness raising information about security. These findings give scope for the development of a technological risk reduction framework to be within MMORPG environments. While popular media stories suggest that the internet is full of predators and any form of online engagement can lead to exploitation, abstinence from certain parts of the internet may be the wrong message. There is an increasing body of thought that points to the value of effective awareness raising .

References

Gladwell, C., Currie, J.. (2009). Online Gaming: Child's Play or Obsession? A Kids Help Phone Online Survey. Retrieved March 11, 2011 from http://org.kidshelpphone.ca/media/53784/online%20gaming%20report%20-%20english.pdf.

Microsoft (2010). Parents are Teaching Their Kids Safer Gaming Habits but More Can Be Done. Retrieved April 11, 2011 from http://www.microsoft.com/security/resources/research.aspx#gaming

Öqvist, K.L.. (2009). Virtual Shadows: Your Privacy in the Information Society. UK: British Computer Society Publishing and Information Products.

Sanders, B.G., Furnell, S.M., Dowland, P.S.. (2009). Online Gaming: An Emerging Avenue for Exploitation?, Proceedings of the Fifth Collaborative Research Symposium on Security, E-learning, Internet and Networking (SEIN 2009), Darmstadt, Germany 25-29 November 2009.

Sanders, B.G., Dowland P.S., Furnell S.M.. (2009). An Assessment of People's Vulnerabilities in Relation to Personal and Sensitive Data, Proceedings of the Third International Symposium on Human Aspects of Information Security & Assurance (HAISA 2009), Athens, Greece.

Yee, Nick. 2003, "Inside Out."Deadalus Project. June 22, 2002. Retrieved on March 31, 2011 from http://www.nickyee.com/daedalus/archives/000523.php.