

Chapter 16

Security Issues in Massively Multiplayer Online Games

Rui Costa Cardoso

Instituto de Telecomunicações, University of Beira Interior, Portugal

Abel Gomes

Instituto de Telecomunicações, University of Beira Interior, Portugal

ABSTRACT

Massively Multiplayer Online Games (MMOGs) have been steadily growing in interest over the past decade. Their economic value turns them into one of the main targets of malware and cheating in Internet. This chapter presents and discusses security issues in MMOG environments. The study starts with a preliminary characterization of MMOGs, highlighting their main features. Afterwards, the authors present the security approaches that are applicable to MMOGs, exposing the implications of security breaches and the need for better protection mechanisms. Next, the chapter presents current safety measures and solutions to tackle specific security issues. Finally, security trends that can be relevant in the future are described.

TARGETED AUDIENCE

The chapter is mainly target to researchers, scholars and game professionals, but also could be of interest to others who are interested in online game security.

INTRODUCTION

The security paradigm that supported game industry for many years was on protecting game software. This was achieved by making difficult

the reproduction of copies of game, so trying to protect game development and investment revenues. Later, with the advent of the Internet, new opportunities arose in the game industry (Jarett, 2003), but this also implied changes in game security. Therefore, while the main security issues of the pre-Internet games were developing copy protection mechanisms, now security is seen in a wider perspective. Currently, online game industry companies obtain most of their profits from pay-to-play solutions, and not from selling games (Yan, 2003).

Basically, MMOG's business model changed with the progressive disappearance of game copies

DOI: 10.4018/978-1-4666-0149-9.ch016

(Chen, 2004), but new problems arose with those pay-to-play solutions (Davis, 2008). In particular, online games and MMOGs put security challenges, namely: security problems related with player authentication, issues related with game availability and resilience, trust and anonymity concerns, means of ensuring security of player and his/her virtual assets, game law enforcing solutions, game client problems (Mönch, 2006), and also game development issues like scalability and persistence. In short, MMOGs share the same security risks as those of other online applications, but also present new and interesting challenges as a consequence of the risks mentioned above.

Despite user's increased awareness in respect to risks of his/her online behavior and, consequently, the inherent security threats, the MMOG player usually has a negligent perception in terms of security. For him/her, it is just another type of online game, where players play anonymously and therefore don't constitute a real threat to him/her and other users. The understanding is that what happens inside game's virtual environment doesn't have consequences in real life. It is clear that this is a wrong understanding in terms of game security and privacy.

There are threats that must be considered when developing and managing MMOG (Davis, 2008). But, many industry developers don't follow this perspective. Due to MMOG business model, whose success results from the amount of players that a game attracts and maintains, a MMOG needs to keep players immersed in the game and luring new ones to allow growth on the number of subscriptions and publicity revenues in order to support the cost of having a computer infrastructure to deploying the game.

Therefore, game's success is a result of what players feel on the game. If the game isn't interesting, it doesn't have an interesting history, it isn't graphically appealing, it has communication lags issues, and there is a sense that the game is unfair and players feel that it is almost impossible to evolve in the game, that there are few players to

interacting with, that they are being scammed, and that they likely lose assets in game due to cheating, that the game doesn't provide a fair dispute resolution to solving game disputes, then players end up leaving the game.

Although some of the previous considerations aren't directly security-dependent, many others are. Therefore game developers must incorporate a well-defined security policy in their business model. In general terms, the success of a MMOG is a corollary on game trust and reliability by players. In fact, the player's perception about security isn't in accordance with the amount of information that he/she shares in a MMOG environment with unknown players (Hogben, 2008). This fact can be used for player profiling and social engineering attacks.

Security in MMOGs goes beyond the security problems of current online applications. The lack of security in MMOGs has implications to user in-game and off-the-game activities. There is a need to promote awareness to security issues within player community, and also to lead game industry to develop better and new security procedures. By identifying the current situation within security in MMOGs, this chapter aims to serve as base for further security research in MMOGs.

This chapter is organized as follows. It starts by briefly describing the game security procedures and their evolution toward online games and MMOGs. Then, we present an overview of MMOGs, with a detailed description of their main characteristics, with a focus on security related features. Relevant security threats, incidents and consequences are then presented, investigated, and analyzed. Afterwards, we present an insight of future measures in the design of new MMOGs that may lead to build up more secure games. The chapter ends with the conclusions, where the main contributions of our research are listed.

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/security-issues-massively-multiplayer-online/64261

Related Content

Feature Extraction Method of Piano Performance Technique Based on Recurrent Neural Network

Zhi Qian (2022). *International Journal of Gaming and Computer-Mediated Simulations* (pp. 1-14).
www.irma-international.org/article/feature-extraction-method-of-piano-performance-technique-based-on-recurrent-neural-network/314589

Nuances of Media Planning in New Media Age

Anandan Pandiyan Pillai (2019). *Application of Gaming in New Media Marketing* (pp. 151-170).
www.irma-international.org/chapter/nuances-of-media-planning-in-new-media-age/211720

Value of a Ludic Simulation in Training First Responders to Manage Blast Incidents

Robert M. Waddington, Thomas C. Reeves, Ellen J. Kalin, William D. Aggen, Marjorie A. Moreau, Harald Scheirich, Jerry Heneghan and Steven Cattrell (2013). *International Journal of Gaming and Computer-Mediated Simulations* (pp. 60-72).
www.irma-international.org/article/value-of-a-ludic-simulation-in-training-first-responders-to-manage-blast-incidents/79936

The Right Kind Of Telling: An Analysis of Feedback and Learning in a Journalism Epistemic Game

David Hatfield (2015). *International Journal of Gaming and Computer-Mediated Simulations* (pp. 1-23).
www.irma-international.org/article/the-right-kind-of-telling/133617

MMORPGs in Support of Learning : Current Trends and Future Uses

Bodi Anderson (2010). *Gaming and Cognition: Theories and Practice from the Learning Sciences* (pp. 55-81).
www.irma-international.org/chapter/mmorp-gs-support-learning/41467