Encyclopedia of Internet Technologies and Applications

Mario Freire
University of Beira Interior, Portugal

Manuela Pereira
University of Beira Interior, Portugal

Information Science
REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Acquisitions Editor:	Kristin Klinger
Development Editor:	Kristin Roth
Senior Managing Editor:	Jennifer Neidig
Managing Editor:	Sara Reed
Copy Editor:	Larissa Vinci and Mike Goldberg
Typesetter:	Amanda Appicello and Jeffrey Ash
Cover Design:	Lisa Tosheff
Printed at:	Yurchak Printing Inc.

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue, Suite 200
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com/reference

and in the United Kingdom by
Information Science Reference (an imprint of IGI Global)
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 0609
Web site: http://www.eurospanonline.com

Library of Congress Cataloging-in-Publication Data

Encyclopedia of Internet technologies and applications / Mario Freire and Manuela Pereira, editors.
p. cm.
Summary: "This book is the single source for information on the world's greatest network, and provides a wealth of information for the average Internet consumer, as well as for experts in the field of networking and Internet technologies. It provides the most thorough examination of Internet technologies and applications for researchers in a variety of related fields"--Provided by publisher.
Includes bibliographical references and index.
ISBN 978-1-59140-993-9 (hardcover) -- ISBN 978-1-59140-994-6 (ebook)
1. Internet--Encyclopedias. I. Freire, Mário Marques, 1969- II. Pereira, Manuela.
TK5105.875.I57E476 2007
004.67'803--dc22
2007024949

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this encyclopedia set is original material. The views expressed in this encyclopedia set are those of the authors, but not necessarily of the publisher.

A Taxonomy of Online Game Security

Kuen Park
Korea University, South Korea

Heejo Lee
Korea University, South Korea

INTRODUCTION OF ONLINE GAME SECURITY

People enjoy playing games for simple pleasure. Recently, since the emergence and advance of the computer technologies, especially in terms of graphic and networking, which enables people to experience virtual world with a computer network they couldn't ever have imagined (Smed & Hakonen, 2003). In this respect, the popularity of games has roared, which builds up the cultural phenomenon because numerous people are involved in the game forming community.

The online game market scale amounted to $19 billion by 2011 (Gamasutra, 2006), which shows that games are not a negligible industry but a Midas's hand, which relates to the other industries such as cinema and music. For instance, the famous game character "Lara Croft" of the game "Tomb Raider" was converted to Hollywood cinema, which was greatly successful.

However, online games face many threats (Chen, Hwang, Song, Yee, & Korba, 2005). An attacker who comprehends the mechanism of online games attempts to lead a game to his favor with malicious actions. This generates unfair advantage for fun or profit (Pritchard, 2001). Online game cheating has not been a simple problem because it is the primary reason an honest player quits the game if he or she had experienced unfair playing from a cheater. Therefore, an online game designer should consider online game security seriously (Yan & Choi, 2002).

This article is constituted as follows. A classification of online games and the associated brief explanations are described with the viewpoint of security. Afterward, a taxonomy of online game attacks and the respective countermeasures are provided. The next section demonstrates how to prepare for predictable game attacks. This article concludes in the final section.

BACKGROUND: ONLINE GAME CLASSIFICATION

Online games have various types of how to attack the game. Thus, game designers should consider the game type about what factors are vulnerable in its game type. Figure 1 represents our classification of online games. Online games can be divided in five categories: abstraction, action, simulation, story-driven, and strategy. The characteristics and security consideration of each game are as follows.

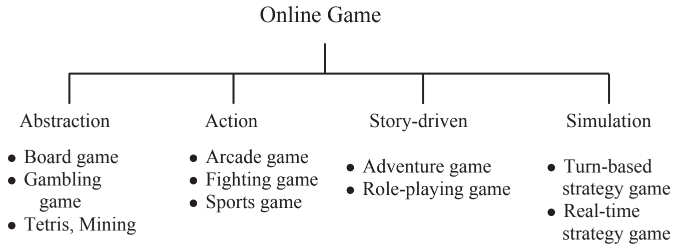
Abstraction Games

Abstraction games represent the game, which is abstracted by the computer programming and its respective design for online gaming. Classical board games and gambling games are often made with some modifications for new rules or fun. Go and chess are good examples of this category. The characteristic of this game type is that it is easy to learn to play than any other game type. Typically, game portal sites such as http://www.hangame.com and http://www.netmarble.com are providing this type of game collectively. In addition, Internet Chess Club (http://www.chessclub.com) is a case for providing this type of game category. A good security analysis of this site is released in 2006 (Black, Cochran, & Gardner, 2006).

Action Games

Action games have genres such as classical arcade, fighting, sports, and FPS games. These kinds of games need fast reactions in the virtual environment. An attacker attempts to modify the related values such as the number of bullets or energy status.

Figure 1. A classification of online games



Story-Driven Games

Story-driven games have two main categories: adventure games and role-playing games. Adventure games focus on resolving specific missions such as quest, mission, or mystery. In role-playing games, the user should make an effort to build his or her character to be stronger with activities. Diablo, Final Fantasy, and World of Warcraft are the representative cases (Griffiths, Davies, & Chappell, 2003).

Simulation Games

Simulation games can be divided into two categories: real-time strategy games and turn-based strategy game. Simulation games focus on careful planning and skillful resource management to achieve victory. In simulation games, resource is the indispensable factor so an attacker tries to alter the amount of resources.

ONLINE GAME SECURITY

Online game attacks can be classified into the following four categories: server attacks, network attacks, client attacks, and user attacks. The respective attacks are briefly introduced in the follow section. Figure 2 shows the classification as a tree format. In the viewpoint of generally accepted security principals and models, we can enumerate online game attacks with respect to three security factors:

- **Confidentiality:** Confidentiality ensures that computer-related assets are accessed only by authorized parties. In this respect, game data attacks harm confidentiality. For maintaining fair online games, confidential information exchange between client and server is necessary.
- **Integrity:** Integrity means that assets can be modified only by authorized parties or in authorized ways. In this context, packet attack and client's four attacks--memory, file, time, and event attacks—are purposed to damage game integrity. If someone can manage packet, memory, file, time, and event, he or she is able to take control of the game on his or her purpose. To protect these values controlled by an attacker, integrity checks should be realized during game play.
- **Availability:** Availability means that assets are accessible to authorized parties at appropriate times. Therefore, DDoS and user attacks damage availability. Someone who transmits overwhelming service requests to the game server can interrupt normal gaming services. In addition, kinds of user attacks disrupt normal item usage of an honest user.

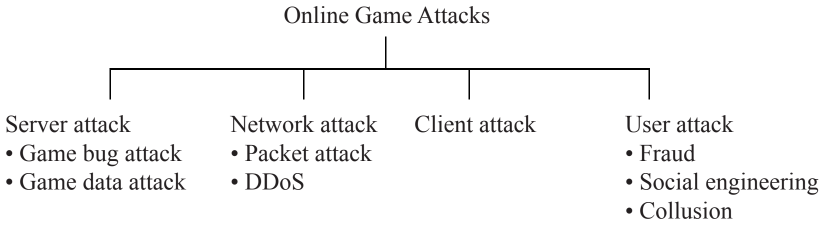
Server Attacks

Game servers contain sensitive data such as ID, password, and game record, which is the main target for an attacker. Game information leakage can be serious damage to the game vendor.

Network Attacks

Online games must interact between server and host via network infrastructure. An attacker can use this property on attack. An attacker can sniff the game packet and fabricate it in his or her favor. Furthermore, he or she can interrupt normal game play with the use of a great number of botnet agents that generate high volumes of traffic.

Figure 2. A classification of online game attacks



Client Attacks

Transforming software file and local environment values such as memory, OS time, and event are the good attacking strategy for an attacker. In addition, numerous auxiliary game hack programs help attackers attack games. These kinds of hack programs have been devised and distributed by hackers for fun or profit.

User Attacks

Because of invisible network gaming environments between users, an attacker can deceive an honest player. For instance, an attacker can obtain an honest user's game information or items by fraud.

SERVER ATTACKS

Game bug attacks represent a game server that has design bugs. An attacker can use it for his or her advantage effectively. For instance, an attacker found a place where he or she may be invisible to an honest user in a certain FPS game. An attacker could kill an honest player only keeping his or her position in the place and shooting the gun when an honest player appeared. In this respect, game server bugs harm the fairness of the game. Therefore, game designers should make effort to cover this kind of vulnerability. Since game data can be transformed into real money, an attacker attempts to fulfill game data attacks. Therefore, an attacker tries to gather items the malicious way. If he or she can take control of server information, he or she is able to transmit items to his or her account and make a profit.

To protect game data attacks, the following set of countermeasures can be adopted. First, data encryption using HTTPS and registry key encryption are recommended prevention. In addition, access control policies should be regularly examined and enforced. Second, OS and DB vulnerability should be checked with OS and DB security tools, which can further check the patch status. Real time backdoor monitoring systems and vulnerability scanning activity can be a good way to protect server attacks. In particular, a trial vulnerability examination is a good way to check and cover the potential threat.

NETWORK ATTACKS

Network attacks to game systems can be divided into two categories: packet manipulation attacks and DDoS. Packet manipulation attacks (Baughman & Levine, 2001) have an objective to reveal the content of game packets. Once an attacker knows its specific meaning, he or she can design packets for his or her favor and transmit them to game server. DDoS attacks are closely coupled with availability that is a main component of computer security. An attacker can attack game systems in order to interrupt normal service using a large number of botnet (Hussain, Heidemann, & Papadopoulos, 2003; Smed, Kaukoranta, & Hakonen, 2001). To prepare for the network attacks, IPS (intrusion prevention system) and its management equipments are dedicated to prevention. Furthermore, network firewall and ACL on router and switch should be examined for DDoS attacks (Dietrich, 2004). SSL VPN and the separation of an internal network with respect to roles can diminish network threats (Merabti & Rhalibi, 2004).

CLIENT ATTACKS

Once an online game is released and it gains popularity, an attacker may start to analyze the game software on the client. After analyzing the software, related auxiliary hacking tools emerge. The hacking tools can be classified as follows:

- **Speedhack (Yan, 2005):** Modifying the time of an game
- **Maphack (wallhack):** Enabling to see game status
- **Memoryhack:** Altering the memory value of an game
- **Packeteditor:** Editing game packets
- **Trainermaker:** Enabling to build customizing hacking functions
- **File patcher:** Replacing game files with hacked files
- **File packer:** Unpacking game files for hacking files
- **Debugger:** Disassembling files to analyze files (Debray, 2005)
- **Gamebot:** Launching programs for automatic item harvesting (Kim, Hong, & Kim, 2005)
- **Bug hack:** Exploits bugs in the game

Secure game designs (Yan, 2003) fundamentally decrease security threats of online gaming. Typically, attackers can analyze game files with reverse engineering. To protect reverse engineering attacks, the code sequence can be obfuscated in a file. In other ways, the integrity checking of game files are highly recommended as an effective defense. In addition, monitoring client game values such as memory, file, time, and event should be required to protect the game variable modification attack. For game client security, various countermeasures can be used. Anti-hack solution is a good way to prevent malicious process communications, which aim to capture targeted memory event. Thus, anti-hack solution can monitor the anomaly situations of game files and game time modification. In addition, the installation of a Web application firewall, which monitors covert channels and traffics for data theft and application disruption, can be an effective countermeasure.

USER ATTACKS

An attacker deceives an honest user to obtain virtual assets using fraud, social engineering, and collusion. Fraud often occurs when exchanging or trading virtual assets. Hence, game designers need to consider the development of a fair trading system that does not allow illegal trading such as taking items but no giving proper rewards. In addition, even if an illegal trading or transaction may occur, a set of procedures that trace swindled items such as a unique ID number for each virtual asset and transaction record system should be prepared. Social engineering represents an attackers' psychological trick on game users in an effort to obtain profitable information or assets (White, 2003). For example, an attacker sends an e-mail disguised as a game administrator requesting a new password and an old password of a user. Collusion occurs when an attacker collaborates with other attackers for the purpose of deceiving honest users to acquire unfair advantages (Murdoch & Zielinski, 2004). In order to avoid collusion, user reputation and reporting systems can be used effectively.

PREPARING FUTURE ATTACKS AND DEFENSES

Anti-Hack Solution File Attack

An attacker tries to modify or delete anti-hack files so that anti-hack cannot operate properly. Some anti-hack solution vendors verify files' integrity; however, the checking module may not always operate correctly. The solution is to check whether anti-hack solution files are impaired during game play.

Skipping Attack

Some anti-hack solutions adopt the policy to check whether an auxiliary client hacking program exists on client with signature-based detection. However, an attacker can skip this check procedure using hot-key based or time-based usage. In particular, delicately devised hacking files are overwritten to real files. Therefore, the anti-hack solution requires monitoring the execution of auxiliary programs during game playing with anomaly detection.

Hardware-Based Gamebot

Current anti-hack solutions are able to distinguish software-based keyboard events and mouse events in order to detect a gamebot for automatic item harvesting. However, hardware-based gamebots can avoid such a detection mechanism. Currently, some gamebot-related vendors distribute many types of hardware-based gamebots for profit, and such commercialized gamebots have gained popularity recently in South Korea. To protect this kind of gamebot, anti-hack solution should encompass the ability to recognize hardware-based gamebots.

CONCLUSION

Online game security is the indispensable factor to determine the market penetration of a game. The pervasive nature of the online game coupled with recent threats makes online game security an area of significant importance. In this article, we have presented a classification of online game attacks and discussed the defense mechanism for four main types of attack. This article confirms that there are several important issues, which requires long-term research attention. The ultimate goal of online game security is to protect games against both known and unknown online game attacks. This ambitious goal cannot be achieved in a single stroke. Therefore, we need to continue the enhancement of online game security in various aspects.

REFERENCES

Baughman, N. E., & Levine B, N. (2001). Cheat-proof playout for centralized and distributed online games. *IEEE INFOCOM*.

Baxter, I. D., & Mehlich, M. (2000). Reverse engineering network: Professional resources for reverse code engineering. *Science of Computer Programming*, *2-3*, 131-147.

Black, J., Cochran, M., & Gardner, R. (2006). A security analysis of the internet chess club. *IEEE Security & Privacy Magazine*, *4*, 46-52.

Carless, S. (2006). Analyst: Online Game Market $13 Billion by 2011. *Gamasutra Industry News.* Retrieved May 17, 2007, from http://www.gamasutra.com/php-bin/news_index.php?story=9610

Chen, Y. C., Hwang J. J., Song, R., Yee, G., & Korba, L. (2005). Online gaming cheating and security issue. In *International Conference on Information Technology: Coding and Computing*.

Griffiths, M, D., Davies, M. N. O., & Chappell, D. (2003). Breaking the stereotype: The case of online gaming. *Cyber Psychology & Behavior*, *6*(1).

Hussain, A., Heidemann, J., & Papadopoulos, C. (2003). A framework for classifying denial of service attacks. *SIGCOMM*.

John, B., Martin, C., & Ryan, G. (2006). A security analysis of the Internet chess club. *Security & Privacy Magazine*, *IEEE*.

Kim, H., Hong, S., & Kim, J. (2005). Detection of auto programs for MMORPGs. *Advances in Artificial Intelligence, 3809, 1281-1284.*

Merabti, M., & Rhalibi, A. E. (2004). Peer-to-peer architecture and protocol for a massively multiplayer online game. *IEEE Globecom Workshops*.

Mirkovic, J., Dietrich, S., Dittrich, D., & Reiher, P. (2004). *Internet denial of service*. Prentice Hall.

Murdoch, S, J., & Zielinski, P. (2004). Covert channels for collusion in online computer games. *Information Hiding, 3200, 355-367.*

Pritchard, M. (2000). How to hurt the hackers: The scoop on Internet cheating and how you can combat it. *Information Security Bulletin.* Retrieved May 17, 2007 from http://www.gamasutra.com/features/20000724/pritchard_pfv.htm

Ruggles, C., Wadley, G., & Gibbs, M. R. (2005). *Online community building techniques used by video game developers*. International Federation for Information Processing.

Smed. J., & Hakonen. H. (2003). *Towards a definition of a computer game.* Turku Centre for Computer Science.

Smed, J., Kaukoranta, T., & Hakonen, H. (2001). Aspects of networking in multiplayer computer games. In

International Conference on Application and Development of Computer Games.

Udupa, S., Debray, S., & Matias, M. (2005). Deobfuscation: Reverse engineering obfuscated code. In *Working Conference on Reverse Engineering*.

White, S, M. (2003). Social engineering. *Engineering of Computer-Based Systems, 1109, 261-267.*

Yan, J. J. (2003). Security design in online games. In *Annual Computer Security Applications Conference*.

Yan, J. J. (2005). A systemic classification of cheating in online games. *Workshop on Network & System Support for Games*.

Yan, J. J., & Choi, H. J. (2002). Security issues in online games. *The Electronic Library*, *20*(2).

KEY TERMS

Anomaly-Based Detection: Anomaly-based detection detects abnormal states, which an attacker provokes.

Anti-Hack Solution: The solution for prevention, detection, and response to the game cheating.

Collusion: An malicious activity between two or more persons to defraud another game user.

Encryption: A procedure that renders the contents of a message or file unintelligible to anyone not authorized to read it.

Gamebot: A program for item harvesting automatically.

Keylogger: A computer program that captures the keystrokes of a computer user and stores them. Modern keyloggers can store additional information, such as images of the user's screen. Most malicious keyloggers send this data to a third party remotely (such as via e-mail).

MMORPG: A massively (or massive) multiplayer online role-playing game or MMORPG is a multiplayer computer role-playing game that enables thousands of players to play in an evolving virtual world at the same time over the Internet.

Online Game: Multiple clients connect a host server through the Internet so that they may play network game.

Signature-Based Detection: Signature-based detection represents a detection method distinguishing the distinctive bit stream from an auxiliary program.