Towards Designing Secure Online Games

Yee, George; Korba, Larry; Song, Ronggong; Chen, Y.-C.

Publisher's version / Version de l'éditeur:

Proceedings of the IEEE 20th International Conference on Advanced Information Networking and Applications (AINA 2006), 2006

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

Towards Designing Secure Online Games *

Yee, G., Korba, L., Song, R., Chen, Y.-C.
April 2006

* published in the Proceedings of the IEEE 20th International Conference on Advanced Information Networking and Applications (AINA 2006). April 18-20, 2006. Vienna, Austria. NRC 48457.

Canada

Towards Designing Secure Online Games[1]

George Yee, Larry Korba, Ronggong Song, and Ying-Chieh Chen
Institute for Information Technology,
National Research Council Canada
{George.Yee, Larry.Korba, Ronggong.Song, Bomy.Chen}@nrc-cnrc.gc.ca

Abstract

The multiplayer gaming industry has become very successful in Asia. With the growth of online gaming, there has been an amazing growth in online gaming-related crime, especially in Massively Multiplayer Online Role-Playing Games (MMORPGs) [1]. In Taiwan, more than 37% of criminal cases relate to online gaming crime with most offenders in the age range of 15-20 years [5]. Most of these crimes can be attributed to the fact that these online games were not designed to be secure. This paper applies a design for security approach to MMORPGs and then examines what crimes could have been avoided if the games were designed to be secure from the beginning. The approach also uncovers some potential new threats and gives countermeasures for them.

1. Introduction

With the prosperity of online gaming, anti-social behaviors and criminal activities have developed concomitantly. In Taiwan, since 2001, many cyber-criminal cases related to online games have occurred, e.g. theft, fraud, robbery, threat, sabotage and others. According to the statistics of the National Police Administration of Taiwan [5], there were 3553 cyber crime cases within which 3983 criminals were prosecuted during 2002. Astonishingly, more than 1300 of these cases were related to online gaming, with online cheating being the most serious criminal behavior.

The design of secure software from the start has been advocated by Viega & McGraw [2] and McGraw [3]. Other researchers have looked at other ways for designing secure software for a particular stage of the software lifecycle or for a particular type of software, or using a particular methodology [4]. Designing secure online games calls for the following steps [2]:

1. Identify potential threats to the online game and how these threats may be carried out.
2. Identify countermeasures to avoid the threats identified in step 1.
3. Use the countermeasures identified in step 2 as security requirements for development.
4. Design and implement the online game, accounting for the security requirements as well as the functional requirements, using secure coding practices.
5. Test the implemented code to make sure security requirements as well as functional requirements are satisfied.

These steps only capture the essence of the design for security approach; however, they serve our purpose, which is not to present design for security in detail but to use it to show that securely designed online games would avoid most of the online gaming crimes experienced. To achieve this purpose, we only need to carry out steps 1 and 2 (also known as threat modeling). We assume that steps 3, 4 and 5 are also done, resulting in an online game that satisfies all the identified security requirements.

We focus on the massively multiplayer online role-playing game or MMORPG (Table 1) since it is the most popular online game in Asia.

Table 1. Characterization of MMORPG

Characteristic	Description
Network Connection	Connected to host server through Internet
Player Authentication	UserID and Password
Game Objectives	Accumulate virtual property through skillful game play to reach game objectives.
Number of Players	A large number of players can all compete with one another playing the same instance of the game.
Payment for Use	Pay for network connection time by buying a card associated with a certain amount of connection time via a serial number on the card.

Section 2 describes threat modeling and builds a threat model for MMORPGs. Section 3 presents a security analysis to identify which online gaming crimes could have been avoided using our approach. Section 4 concludes the paper.

2. Threat modeling for MMORPG

Threat modeling or threat analysis is a method for systematically assessing and documenting the security risks associated with a system [6]. The results can help development teams identify the strengths and weaknesses of the system and serve as a basis for investigations into vulnerabilities and required mitigation. Threat modeling involves understanding the adversary's goals in attacking the system based on the system's assets of interest.

Method

The method used here for threat modeling is based on [6], consisting of the following steps: 1) identify threats, 2) create attack trees for the system, 3) apply weights to the leaves, 4) prune the tree so that only exploitable leaves remain, and 5) generate corresponding countermeasures.

Step 1: Identify threats

By considering the characteristics of a MMORPG system (Table 1), we arrive at the following list of potential threats from an adversary:

- Gain illegal access to play the game
- Cheat at game play
- Disrupt game play
- Cheat at paying for game play
- Steal proprietary parts of the software

Steps 2, 3, and 4: Create attack trees, apply weights, and prune

The 5 attack trees corresponding to the threats of step 1 together with their weighting, and pruning follow. The weighting of each leaf is denoted by a triple (risk, access, cost) where each member of the triple has values H (high), M (medium), and L (low). Pruned nodes are indicated using grey highlighting. Deciding which nodes may be pruned depends in part on the level of fanaticism to which game players can be pushed in the "heat of the moment". The higher this level, the more risk and cost the adversary is willing to bear. Since experience shows that this level can be very high for Asians playing MMORPGs, we chose to prune nodes with combinations of M's and at least one H to reflect a high tolerance for risk and cost.

1. Gain illegal access to play the game

1.1. Use someone else's password (userid known)
- *1.1.1. Acquire by robbery (H, L, L)*
- *1.1.2. Guess password (L, L, L)*
- *1.1.3. Dictionary attack on password (L, L, L)*
- *1.1.4. Use Trojans to acquire password (L, L, L)*
- *1.1.5. Use social engineering to acquire password (M, L, L)*
- *1.1.6. Use man-in-the-middle attack to capture userid and password*
  - *1.1.6.1. Capture information at a router (L, M, M)*
  - *1.1.6.2. Capture information on a link (L, M, M)*

1.2. Inside job arranges free access
- *1.2.1. Bribe unscrupulous insider (M, M, H)*
- *1.2.2. Force insider cooperation using personal threat (H, L, L)*
- *1.2.3. Insider takes revenge on company for some perceived injustice (L, M, L)*

1.3. Attack on authentication software
- *1.3.1. Disable software using secret backdoor (L, M, M)*
- *1.3.2. Disable software using secret vulnerability (L, M, M)*

1.4. Phishing for userid and password
- *1.4.1. Use fake website (M, L, L)*
- *1.4.2. Use fake email to trick player into giving up password (userid known) (M, L, L)*

2. Cheat at game play

2.1. Collude with others to attain higher levels of play
- *2.1.1. Obtain others' cooperation for mutual benefit (M, L, L)*
- *2.1.2. Pay others to cooperate against another game player (M, L, M)*
- *2.1.3. Force others to cooperate using personal threat (H, L, L)*

2.2. Use cheat program
- *2.2.1. Program makes it easier to attain higher levels (L, M, M)*
- *2.2.2. Program acts for the player, playing game faster with greater accuracy (L, M, M)*

2.3. Buy virtual properties/skill
- *2.3.1. Buy virtual property from others for transfer to own game profile (L, L, H)*
- *2.3.2. Pay "champion level" players to play on own game account (L, L, H)*

2.4. Steal virtual properties/skill
- *2.4.1. Obtain virtual property by robbery (H, L, L)*
- *2.4.2. Force "champion level" players to play on own game account using personal threat (H, L, L)*

2.5. Inside job arranges for player to easily attain high levels
- *2.5.1. Bribe unscrupulous insider (M, M, H)*
- *2.5.2. Force insider cooperation using personal threat (H, L, L)*

2.6. Attack on gaming software that controls play levels
- *2.6.1. Modify software using secret backdoor (L, M, M)*

2.6.2. *Disable software using secret vulnerability (L, M, M)*

3. Disrupt game play

3.1. Man-in-the-middle attack on communications

3.1.1. Intercept traffic at router and substitute bad traffic (M, H, M)

3.1.2. Intercept traffic on link and substitute bad traffic (L, L, M)

3.2. DNS (denial of service) attack

3.2.1. DNS attack on server disrupting game for all players (L, L, L)

3.2.2. DNS attack on specific link or router disrupting game for particular players (L, L, L)

3.3. Inside job arranges disruptions

3.3.1. Bribe unscrupulous insider (M, M, H)

3.3.2. Force insider cooperation using personal threat (H, L, L)

3.3.3. Insider takes revenge on company for some perceived injustice (L, M, L)

3.4. Release virus/worms

3.4.1. Release virus/worms across entire system (M, L, L)

3.4.2. Release virus/worms to target specific players (M, L, L)

3.4.3. Release virus/worms to target server (M, L, L)

4. Cheat at paying for game play

4.1. Obtain copies of legitimate time card serial numbers

4.1.1. Inside job at card manufacturer or transporter or distributor/retailer

4.1.1.1. Bribe unscrupulous insider (M, M, H)

4.1.1.2. Force insider cooperation using personal threat (H, L, L)

4.1.2. Inside job at game provider

4.1.2.1. Bribe unscrupulous insider (M, M, H)

4.1.2.2. Force insider cooperation using personal threat (H, L, L)

4.1.2.3. Insider takes revenge on company for some perceived injustice (L, M, L)

4.1.3. Obtain card by robbery (H, L, L)

4.1.4. Dictionary attack on time card serial number (L, L, L)

4.1.5. Guess time card serial number (L, L, L)

4.1.6. Use Trojans to transmit a player's time card number (L, L, L)

4.2. Attack on connection time tracker software

4.2.1. Disable software using secret backdoor (L, M, M)

4.2.2. Disable software using secret vulnerability (L, M, M)

4.3. Inside job at game provider arranges for free time (other than providing time card serial numbers)

4.3.1. Bribe unscrupulous insider (M, M, H)

4.3.2. Force insider cooperation using personal threat (H, L, L)

4.3.3. Insider takes revenge on company for some perceived injustice (L, M, L)

5. Steal proprietary parts of the software

5.1. Inside job arranges theft

5.1.1. Bribe unscrupulous insider (M, M, H)

5.1.2. Force insider cooperation using personal threat (H, L, L)

5.1.3. Insider takes revenge on company for some perceived injustice (L, M, L)

5.2. Attack on server containing desired software

5.2.1. Illegally enter premise and copy code (H, M, M)

5.2.2. Hack into server and copy code (L, M, L)

5.3. Use Trojans to transmit desired code or design documents (L, L, L)

5.4. Use social engineering to acquire proprietary information (M, M, L)

5.5. Kidnap members of design team (H, M, M)

Step 5: Generate corresponding countermeasures

Table 2 lists our proposed countermeasures for each attack path in the pruned attack trees.

Table 2. Attack path countermeasures

Attack Path	Countermeasure
1, 1.1, 1.1.1	Better authentication perhaps using biometrics – difficult to defend if the criminal is desperate enough (e.g. forced biometric sign-in)
1, 1.1, 1.1.2	Lock user out after 3 tries
1, 1.1, 1.1.3	Lock user out after 3 tries
1, 1.1, 1.1.4	Scan and eliminate all malware
1, 1.1, 1.1.5	Require strict procedures for information disclosure
1, 1.1, 1.1.6, 1.1.6.1	Use secure channel (e.g. SSL or VPN) for communications
1, 1.1, 1.1.6, 1.1.6.2	Use secure channel (e.g. SSL or VPN) for communications
1, 1.2, 1.2.2	Increase physical security and penalties
1, 1.2, 1.2.3	Increase organizational sensitivity to employees; improve organizational management and communication with employees
1, 1.3, 1.3.1	Employees put in backdoors out of feelings of insecurity, same remedy as path 1.2, 1.2.3
1, 1.3, 1.3.2	Use secure coding practices
1, 1.4, 1.4.1	Authenticate website using digital signature
1,1.4, 1.4.2	Authenticate email using digital signature
2, 2.1, 2.1.1	Should this really be illegal?
2, 2.1, 2.1.2	Should this really be illegal?
2, 2.1, 2.1.3	Educate game players against this type of crime and install better police procedures

2, 2.2, 2.2.1	Cheat programs rely on software backdoors or vulnerabilities. Apply countermeasures for 1, 1.3, 1.3.1 and 1, 1.3, 1.3.2
2, 2.2, 2.2.2	Same as for 2, 2.2, 2.2.1
2, 2.3, 2.3.1	Should this really be illegal?
2, 2.3, 2.3.2	Should this really be illegal?
2, 2.4, 2.4.1	Watermark virtual property together with police investigation
2, 2.4, 2.4.2	Increase physical security and penalties
2, 2.5, 2.5.2	Increase physical security and penalties
2, 2.6, 2.6.1	Same as for 1, 1.3, 1.3.1
2, 2.6, 2.6.2	Same as for 1, 1.3, 1.3.2
3, 3.1, 3.1.2	Increase link physical security or increase route diversity to bypass the compromised link. Information security methods (e.g. hashing) would not prevent disruption.
3, 3.2, 3.2.1	Use DNS attacker detection methods; use alternate servers as back-up.
3, 3.2, 3.2.2	Use DNS attacker detection methods; use route diversity to switch players to other routes.
3, 3.3, 3.3.2	Same as for 1, 1.2, 1.2.2
3, 3.3, 3.3.3	Same as for 1, 1.2, 1.2.3
3, 3.4, 3.4.1	Use virus/worm detection software but damage may already have occurred. This is difficult to defend against.
3, 3.4, 3.4.2	Same as for 3, 3.4, 3.4.1
3, 3.4, 3.4.3	Same as for 3, 3.4, 3.4.1
4, 4.1, 4.1.1, 4.1.1.2	Same as for 1, 1.2, 1.2.2
4, 4.1, 4.1.2, 4.1.2.2	Same as for 1, 1.2, 1.2.2
4, 4.1, 4.1.2, 4.1.2.3	Same as for 1, 1.2, 1.2.3
4, 4.1, 4.1.3	Invalidate card if robbery known. Otherwise, increase physical security and do frequent card inventories.
4, 4.1, 4.1.4	Same as for 1, 1.1, 1.1.2
4, 4.1, 4.1.5	Same as for 1, 1.1, 1.1.2
4, 4.1, 4.1.6	Same as for 1, 1.1, 1.1.4
4, 4.2, 4.2.1	Same as for 1, 1.3, 1.3.1
4, 4.2, 4.2.2	Same as for 1, 1.3, 1.3.2
4, 4.3, 4.3.2	Same as for 1, 1.2, 1.2.2
4, 4.3, 4.3.3	Same as for 1, 1.2, 1.2.3
5, 5.1, 5.1.2	Same as for 1, 1.2, 1.2.2
5, 5.1, 5.1.3	Same as for 1, 1.2, 1.2.3
5, 5.2, 5.2.2	Use a combination of firewall and intrusion detection; as well, use obfuscation on the executables.
5, 5.3	Same as for 1, 1.1, 1.1.4
5, 5.4	Same as for 1, 1.1, 1.1.5

As can be seen, the above countermeasures include physical security remedies as well as information security solutions. They are not the only countermeasures that may be applied. In addition, some of the attacks should perhaps not be considered as attacks (e.g. 2, 2.1, 2.1.1), depending on the rules of game play and what people may be naturally inclined to do (as long as no laws are broken).

3. Security analysis of secure MMORPG vs. observed crimes

We now examine the observed crimes given by Yan & Choi [7] (first 11 below) and Chen et al [8] (last 6 below) to see which of these crimes our countermeasures cover (indicated in italics).

1. Fraud by Collusion: *Not covered due to unclear rules of game play prior to threat modeling.*
2. Fraud by Alliance: In some MMORPG series, players can build their own team or group with other players so as to share their virtual properties for the purpose of efficiently upgrading levels. *Not clear that this must be illegal. For example, the rules of game play could allow this but specify that the team or group size must be no larger than some fixed number.*
3. Fraud by Abusing Policy: In some gaming systems or websites, statistical mechanisms may be used to record every win and loss in the server. In order to avoid a loss being recorded, the player may disconnect the network before the game ends and the loss recorded, thereby allowing the player to keep his former ranking. *Not covered but this appears to be a give-away, a design fault that allows players this option. This is not a fraud like the others.*
4. Cheating Related to Virtual Property: In most cases, virtual property is the target of criminal activity. *Covered (2.4.1). Note: 2.4.1 (leaf) uniquely identifies the countermeasure in Table 2.*
5. Fraud by Compromising Password: UserID and password combinations are the keys to the virtual online gaming world. *Covered (1.1.x, 1.1.6.x). Note: 1.1.x means any leaf 1.1.1, 1.1.2, etc. Similarly for 1.1.6.x.*
6. Fraud by Denying Service to Peer Players: In some online tournaments, players may use denial of service (DOS) attacks against their online opponents in order to gain advantage in the game. *Covered (3.2.2).*
7. Fraud due to Lack of Authentication: More than 90% of online games merely use UserID and password to authenticate their players. A fake server, compromised DNS server, or fake webpage may serve to steal a player's identity. *Covered (1.4.x).*

8. Fraud-Related Internal Misuse: The employee of an online gaming company may modify the values or parameters of virtual characters through their server in order to gain an illicit advantage. They may also steal a customer's UserIDs and passwords, credit card numbers or related private data for economic profit. *Not covered – that an insider would commit this fraud for his/her own benefit was not considered.*
9. Fraud by Social Engineering: Social engineering was used in more than 26% of cases we have studied. *Covered (1.1.5, 5.4).*
10. Fraud by Modifying Game Software or Data: Cheaters may use reverse engineering, diagnosis tools, memory scanning tools, proxy servers, or cheating programs to modify the results of the game in order to gain illegal advantage. *Covered (2.2.x, 2.6.x).*
11. Fraud by Exploiting Bugs or Design Flaws: Cheaters exploit a bug or design flaw to get unfair or illegal advantage. *Covered (2.2.x, 2.6.x).*
12. Fraud by Trade or Exchange: A cheater might broadcast fraudulent trading information through an auction website, email, BBS, or a chat window within the game. They trick buyers to transfer money to the cheater's bank account. *Not covered.*
13. Fraud by Identity Theft: *Covered (all countermeasures for Attack Tree 1).*
14. Cheating the Online Gaming Vendor: Cheaters pretend that they have forgotten their UserID or password and then ask the vendor for them. However, a UserID and password may have been sold or transferred beforehand. *Covered (1.1.1).*
15. Fraud by Sharing UserID and Password: Some players like to share their UserID and password with friends or relatives as a way to reach a certain level more rapidly through cooperation. *Not clear that this must be illegal – depends on the purpose of reaching the level (e.g. win $1 million or just for personal gratification). If illegal, it is covered (1.1.1).*
16. Fraud due to Lack of Secrecy: Cheaters can exploit network monitoring tools to intercept or eavesdrop on the network packets. *Covered (1.1.6.x).*
17. Fraud by Faking Official Website (Phishing): *Covered (1.4.1).*

4. Conclusions

The above analysis shows that by developing a secure MMORPG system, 12 out of 17 (70.6 %) threat risks to the system have been significantly reduced through the use of countermeasures. Of the 5 threats that were not covered by the countermeasures, threat number 12 is due to human behavior that was difficult to foresee, threat number 8 was an oversight of threat modeling, threat number 3 almost doesn't count because it was a design give-away, and threat numbers 1 and 2 were not modeled due to lack of clarity concerning the rules of game play.

In addition, the design for security approach has put in place countermeasures for new threats that are not part of the 17 crimes or threats from [7, 8]. Some of these new threats are a) insider attacks to get revenge on the company, b) disrupting game play by intercepting traffic and injecting bad traffic, c) attacks to get legitimate time card serial numbers, d) attacks on connection time tracker software, and e) attacks to steal proprietary parts of the software. This shows that the design for security approach can prepare for threats that adversaries have not yet considered (but will consider eventually).

References

[1] Y.C. Chen, P.S. Chen, G. Yee, R. Song, L. Korba, "Online Gaming Cheating and Security Issue", Proceedings, International Conference on Information Technology Coding and Computing (ITCC 2005), Las Vegas, NV, USA, April 4-6, 2005.

[2] J. Viega and G. McGraw, "Building Secure Software", Addison-Wesley, 2002.

[3] G. McGraw, "Building secure software: better than protecting bad software", IEEE Software, Volume 19, Issue 6, Nov.-Dec. 2002.

[4] G. Yee, "Recent Research in Secure Software", unpublished report, available as of Jan. 20, 2006 from: http://www.georgeyee.ca

[5] National Police Administration Publication, "Annual Criminal Statistics Report", Taiwan, 2003.

[6] C. Salter, O. Sami Saydjari, B. Schneier, J. Wallner, "Towards a Secure System Engineering Methodology", Proceedings of New Security Paradigms Workshop, Sept. 1998.

[7] J. J. Yan and H. J. Choi, "Security issues in online games", The Electronic Library, Vol. 20, No. 2, 2002.

[8] Y. C. Chen, P. S. Chen, R. Song, G. Yee, and L. Korba, "Classification of Online Gaming Crime and Security", IRMA 2005 International Conference, San Diego, California, USA, May 2005.

[1] NRC Paper Number: NRC 48457