Online Gaming Crime and Security Issue - Cases and Countermeasures from Taiwan

Chen, Y.-C.; Chen, P.; Song, Ronggong; Korba, Larry

Publisher's version / Version de l'éditeur:

Proceedings of the 2nd Annual Conference on Privacy, Security and Trust (PST'2004), 2004

National Research
Council Canada

Conseil national
de recherches Canada

Institute for
Information Technology

Institut de technologie
de l'information

NRC-CNRC

*Online Gaming Crime and Security Issue - Cases and Countermeasures from Taiwan **

Chen, Y.-C., Chen, P., Song, R., and Korba, L.
October 2004

* published in the Proceedings of the 2nd Annual Conference on Privacy, Security and Trust. Fredericton, New Brunswick, Canada. October 13-15, 2004. NRC 47401.

Canada

Online Gaming Crime and Security Issue – Cases and Countermeasures from Taiwan

Ying-Chieh Chen, Patrick S. Chen, Ronggong Song, Larry Korba

***Abstract*—Along with the growth of information technology, online gaming has become a very successful and outstanding industry recently, especially in Asia. However due to the lack of legal regulation, security protection, privacy protection and related legislation, more and more players (mostly in the age range of 15-20) have violated the law. A fair number of arrests and prosecutions have occurred related to this. Online gaming is designed for entertainment. However, the cyber-criminal activity arising from online games is increasing at an alarming rate. The numbers of thefts, frauds, robberies, counterfeited documents, vandalisms, threats and illegal gambling cases from online gaming have increased to 1300 cases from 55 only 2 years earlier in Taiwan. In fact, some of these cases involved school dropouts who formed malicious gangs to boost their criminal activity. In other words, online gaming contributes to the increasing number of cyber-crimes, to such an extent that it is the number one cyber-criminal activity in Taiwan (in terms of convictions). More recently, all types of network-related crimes have increased rapidly. As well, the average age of players has decreased. The main objective of our research was to find a way to solve these problems.**

***Index Terms*—online gaming, cybercrime, prosecution, privacy, virtual community**

I. Introduction

ONLINE gaming (or massively multiplayer online role-playing game, MMORPG) is a form of computer entertainment played by one or more persons over the Internet. According to the forecast of DataMonitor.com, the global online gaming market will present $3.2 billion and 113 million users in 2005 [1]. It is an explosive technology and has made a very successful business in Asia recently. Many online gaming companies in Asia are not surviving but thriving. For instance, the online gaming “Lineage”, which was developed by NCSoft.com of Korea, made about 133 million U.S. dollars profits in 2002, and reached US 144 million dollars by 2003 [2]. The online gaming in Asia can be called the most successful software industry. There were about 2.03 million players in South Korea in 2002 and more than 2 million players in Taiwan in 2003 [3], which was almost one-fourth the network user population of Korea and Taiwan. The success of online gaming changes the software business model, and makes the related industry have a prosperous growth, for example, broadband network, online payment, internet café, advertising and so on. Furthermore, many vendors from Asia target their products towards North America, Europe, etc., and we can see that online gaming is beginning to take off and thrive in many countries. Nevertheless, what we are concerned about the accompanying negative influence of on e-society.

Along with the emergence of online gaming, many problems have risen and greatly influenced our society. Before the era of online gaming, computer games were single-player against a computer opponent itself. Win or lose, the game’s outcome would not have a serious affect on players. Unlike the traditional computer gaming, online gaming players have been able to compete against or cooperate with real human players, thus influencing them. The “I can see you, and you can see me” principle makes online gaming more interactive and exciting. In the virtual world of online games, players can build their own virtual community, set them free from the confinement of the real world and insert various multimedia, graphic effect, etc. As well, they can play whatever roles they like. The virtual society that imitates the real world may provide interactions, markets, stores, hotels, restaurants, transportation, virtual money, weapons and so on. However, these virtual properties in the virtual society may have a very high value. For example, according to the auction website from Yahoo; the level nine virtual knife is worth more than US $1000 dollars [4]. As another example, consider Korea’s Lineage game, the virtual currency exchange rate was 2500:1 (2500 virtual currency can be converted to 1 US dollar) during 2002. Many players are willing to pay real money to buy virtual property in order to upgrade their virtual characters. These have led many players to attempt to benefit from the illegal use of online virtual properties through online cheating, theft, robbery, and so on.

The remainder of this paper is organized as follows. In section II, we will take a glance at online gaming definition and define our research scope. As well, current online gaming business and status are briefly reviewed in this section. In section III, the forming of virtual communities will be reviewed. Subsequently, in section IV, we will discuss the online gaming crime including its virtual property, criminal dilemmas, and anti-social behaviors. In section V, we present

Ying-Chieh Chen is with the Information Management Department, National Chiao-Tung University, Taiwan, and he is now with the Information Security Group, Institute of Information Technology, NRC, Canada. (e-mail: bomy.chen@nrc.ca)

Patrick S. Chen is with the Information Management Department, Central Police University, Taiwan. (e-mail: chenps@sun4.cpu.edu.tw)

Ronggong Song is with the Information Security Group, Institute of Information Technology, NRC, Canada. (e-mail:ronggong.song@nrc.ca)

Larry Korba is with the Information Security Group, Institute of Information Technology, NRC, Canada. (e-mail:larry.korba@nrc.ca)

possible countermeasures for the prevention of online gaming crime. Finally, we give our concluding remarks in Section VI.

II. ONLINE GAMING

In this Section, we illustrate the online gaming definition and discuss the online gaming business model and technical model since they are important factors to make online gaming thrive in Asia. Then, we review the latest globe marketing of online gaming.

A. *Online Gaming Definition*

Online gaming or online games are the games that are played online via the LAN, Internet, or even Telecommunication. They are distinct from video and computer games that are not networked. Normally, all technical requirement for playing online games is a web browser and/or appropriate client software. A game played in a browser is called a browser-based game or web game. In broad definition, online gaming includes Internet gaming, web gaming, online gambling, local LAN gaming, and mobile gaming, but not the non-networked video and personal computer gaming. Figure 1 illustrates the different types of online games. Within the diagram, the overlapping circles such as MMORPG, Internet, Web and online gambling games are generally operated through wide/public network environment. Mobile gaming is operated by telecommunication, and local LAN gaming is operated by local/private network.

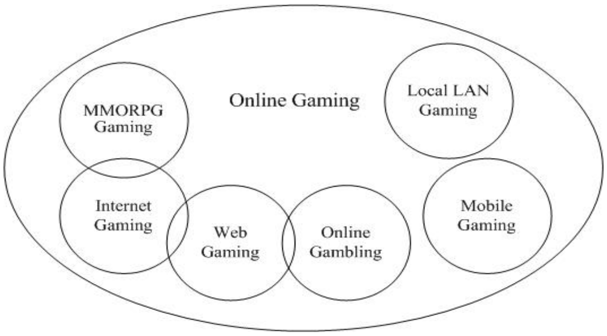

Fig. 1. The different kinds of online games

B. *Online Gaming Business Models*

Currently within MMORPGs, most online gaming operations can be categorized into three business models. These are described as follows.

1) Model 1 – Charge for Software License

This is the traditional business model, i.e. game companies earn profits by selling their software license as boxed product. Players only need to pay once in order to use the software and network connection. In this model, some companies even provide network connection functionality but the players do not need to pay extra money for the online components. Examples of such gaming software are Bizzard's Diablo and Microsoft's Empire. In this situation, software piracy is the main concern for the vendors. Relevant regulations are contained in the copyright laws. The ability to connect to other players over the Internet or LAN is considered value-added for customers, so the customers can choose single or multiplayer mode. Actually, many vendors don't have a strong contract with their online customers or a systematic auditing mechanism for their servers. If customers lodge complaints with respect to their virtual assets, recovery of previous backup or even ignorance is the common reaction taken by vendors. When disputes arise, the vendors take very little responsibility for their online consumers in terms of protecting or managing their virtual property. This attitude taken by the vendors is due to the fact that network connection is a free or value-added service for their online consumers.

2) Model 2 – Charge for Network Connection

Since 2000, the "charge for network connection" model has become the most successful business model. It has created enormous profit and market value, especially in many Asian countries. This model was chosen to improve profit amidst the serious pirating problem. In this model, the vendors freely (or charge very little) distribute their client software (games) from websites or retail channels, so the copyright of software is not the major issue. Unlike charging for software license, the vendors earn profits from selling their service, since customers can only play the games by logging onto the vendor's server. In general, this model calls for more legal contracts and obligations between vendors and players. The vendors are supposed to help consumers maintain players' benefits and solve their problems as soon as their rights or benefits are affected.

3) Model 3 – Charge for Software License and Network Connection

Players must purchase the game software at retail, and also pay a certain amount to play online. Vendors get income both from the retail channel and their online connections; therefore, this model has the utmost advantages than the other models. Example games in this category are Ultima Online [5] and Everquest [6]. However, from the player's perspective, the expensive fee is a deterrent to playing such games.

III. VIRTUAL COMMUNITY FORMING

A strong and tight virtual community has evolved from online gaming in the same way that communities form in the real world. Since interaction is an important part in online gaming, players can build virtual relationships with other players that have the same objectives and hobbies. The genuine understanding and experience sharing between players or allies become the foundation of virtual community with many characteristics similar to the real world in terms of honesty, devotion, positivity, enthusiasm, and so on [7]. The virtual community can be built with diversity, unity, and reciprocity. For instance, in the case of diversity, the players would have different backgrounds but share common ideas, mindsets, interests, curiosities and hobbies, and so on. In the case of unity, they would have same objectives and aspirations, cooperating with one another in order to reach their goals. Based on the diversity and unity, reciprocity would help them make long term relationships and result in cohesion.

On the other hand, the virtual world allows players to do things that they are not allowed to do in the real world. This truth is reflected in MMORPGs. For example, when someone is assaulted by another player's character, this victim might call his/her friends for help. The friends might fight back, attack, or rob the offender's virtual property or even cash, for revenge, all taken for granted. For teenagers, online gaming allows them to do things that they don't dare do in the real world. Most players are youngsters and lack the ability to control themselves, and are easily affected by their peers. Along with these anti-social and criminal aspects, many other negative issues appear concerning online gaming activities: addiction, aggressive behavior, decrease in intelligence, and promotion of gender biases and stereotyping [8]. Therefore, we should take online gaming seriously. Sociologists, enforcement authorities, teachers, and parents are indeed worrying about the problems stemming from online gaming. Violence-oriented online games affect young people both mentally and physically.

In addition, online gaming is nothing but entertainment in one sense, but in a subjective sense, reflects the time, effort, money, and affections that players have been invested in their online games. Once a player's virtual property is gone; then follows suffering, heartbreak, depression, or even suicide, sometimes unbelievable and unimaginable for an outsider. Without the study of online gaming, it is difficult to understand how it influences our teenagers and how it causes anger and frustration just because of virtual property theft. Actually, both victims and offenders understand precisely the value of UserIDs, passwords, points, virtual money and virtual assets.

IV. Online Gaming Crime

In this Section, we will first introduce the creation of virtual property within the online gaming systems, and then analyze the associated online gaming crimes.

A. *Virtual Property*

In MMORPGs, players have to pay a network connection fee for operating their virtual character; in the meanwhile, related valuable virtual parameters accumulate. Therefore, the value of a gaming UserID is unquestionable. Since the number of virtual properties is limited and some virtual equipment cost time and energy for developing, some players who need these assets would like to trade for them. This causes some virtual properties to have very high values in the marketplace. Take the Lineage II online game for instance, for which it depicts a 57 level ranger UserID valued at $2000 U.S. dollars in an Ebay auction website [9]. In ItemBay.com, more than 21,907 related virtual properties of online gaming were sold, bought, or bid for in a an auction website [10]. Moreover, a virtual dragon knife was bid $4,800 U.S.; a royally invincible claw was bid $4,270 [11]. Even the virtual currency in an online game can be converted into cash through exchange with other players. The virtual currency exchange rate was 2500:1 (2500 virtual currency can be converted to 1 US dollar) in the August of 2002 and 10000:1 in March 2003. These facts indicate that virtual property trading is indeed prosperous and flourishing.

This trading of virtual property has become part of the entertainment pleasure, experience, and common practice. We can trace this back to online games such as Sony's EverQuest [6] and Bizzard's Diablo [12]. Players using cash to purchase virtual property can save time and promptly upgrade their virtual skills or levels of play. Some players run their business to assist others players to reach a certain level (e.g. Lineage II) and reaching level 28 within 3 to 4 days requires $113, reaching level 50 within 15 to 20 days requires $945, and so on [13]. Online gaming has evaluated various trading models and methods. It is unlikely that vendors will revise the rules in order to eliminate trading. Players who want to trade virtual property can utilize varied trading channels to sell, purchase, or make exchanges. For solving these trading dilemmas, ItemBay.com [10] was established in 2001 to provide a trading platform for players who want to exchange, sell, or purchase virtual properties in Korea and Taiwan. Under ItemBay.com, more and more players can earn profits from online gaming without taking undue risk. When virtual properties become valuable in the real world, online game is no longer just entertainment. The involvement of real money can easily lead to conflicts of profit and resulting criminal behaviors.

B. *Criminal Dilemma and Influence*

With the prosperity of online gaming, the criminal problems and anti-social behaviors are also quickly developing. 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 [14], there were 3553 cybercrime cases for which 3983 criminals were prosecuted during 2002. Astonishingly, within these cases, more than 1300 were related to online gaming representing almost 37% of all cybercrime cases. At this point it is best to consider the online gaming cases as a separate breed of cybercrime. These criminal developments raised concern among many people; on the other hand, such criminal activities occurred in many Asian countries. Among the cases prosecuted, online cheating is the most serious criminal behavior.

Since the UserID means everything owned by players in the virtual world, hackers have aimed at the UserID and password and tried their best to compromise them. Usually, the hacker would first spam Trojan horse programs or cheat code through Email, malicious websites, FTP sites, plug-in software, cheating programs and so on, or even hide the Trojan in the public computers of an Internet café in order to illegally obtain UserIDs and passwords. After acquiring a

UserID and password, the hacker can obtain much profit using them to do almost anything, for example, use the victim's identity to cheat the victim's friends for virtual property, money, treasures, or equipments, or steal/resell virtual properties.

There are also many ways that have been publicized to cheat players of online gaming. Most players would not know the kind of cheating programs that have been used unless the programs have been publicized or patch programs have been applied by the vendor. Knut Hakon categorizes cheating into 5 stages [15], i.e. unknown cheat, known cheats being exploited by few, known cheats with no patches known within a large group, known cheats with patches, and known cheats with patches applied. In Knut Hakon's definition, an unknown cheat stage is stayed none risk level, but it possibly may cause minor risk to other users as well as the stage of known cheats with patches applied. After our improvement, Figure 2 shows the 5 stages referring to its risk level from minor to large then to minor finally. In this diagram, it also shows the risk reaching the highest level when the cheat is known with patches. In other word, the majority of players have already been cheated by the time the vendor announces a patch program to prevent the cheat.

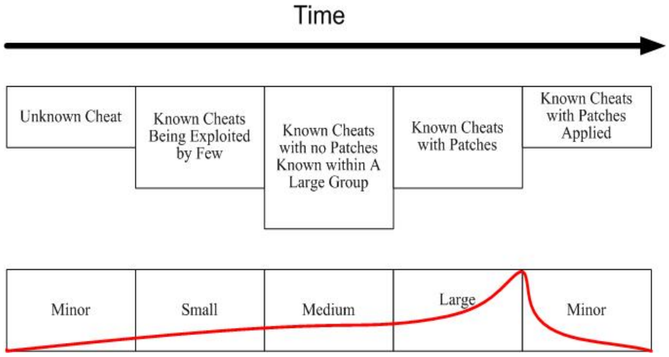
Time
Unknown Cheat
Known Cheats Being Exploited by Few
Known Cheats with no Patches Known within A Large Group
Known Cheats with Patches
Known Cheats with Patches Applied
Minor
Small
Medium
Large
Minor

Fig. 2. Risk of online cheating

From the above, it is clear that there is a growing number of players who are apparently more interested in gaining profit from the online games rather than just being entertained. Many cheating programs including Trojan horse, hacking tools or unauthorized plug-in software are available to the public. These software packages provide a quick, easy, and dishonest way to achieve players' desires within the game. Some players also exploit software defects in online games to cheat other players and gain virtual fortunes. In the well-known case of Blizzard's Diablo [13], due to online cheating problems many players chose to quit this series of games and to play console or local LAN connections only with trusted friends. Currently, the situation has worsened for many online games, like Jin-Yong online [16], Three Kingdoms online [17], MU online [18], Everquest [7], and CrossGate [19]. A website which provides many kinds of cheating programs for online gaming, provides more than 1900 different kinds of cheating programs have been made to attack gaming memory and modify for more than 61 online games while they are running [20]. Through the powerful distribution of the Internet, online cheating using these cheating programs, hacking tools and unauthorized plug-in software are now gradually undermining the gaming industry.

Many criminal dilemmas and anti-social behaviors have emerged in an endless stream. The following news events may be shocking. According to the statistics of the United Daily News newspaper in Taiwan, about 200 online gaming criminal cases were happening every day totaling to at least 50,000 cases every year [21]. One girl was defrauded about US$ 42,000 on her virtual property trading [22]. One report from Hankyoreh.com of South Korea mentioned that a cheater, who was caught in May 2001, had earned more than US$ 11,000 by cheating in online gaming [23]. Police hunted down an offender who developed and distributed illegal cheating programs in China and found over 30,000 detailed UserIDs and passwords [24]. Virtual properties belonging to twenty players were stolen in an Internet café simultaneously due to UserID and password hacking [25]. Offenders kidnapped two players and force them to speak out their UserIDs and passwords; afterwards, they stole all the virtual properties to their victim [26]. Some offenders installed hidden cameras in Internet cafés in order to monitor and steal UserIDs and passwords. There were several cases of players fighting for revenge on the street, because one of their virtual characters had been killed or had some conflicts during game play [27]. An employee who worked in an online gaming company modified a server parameter in order to gain profit from selling those virtual properties [28]. With the increase in criminal cases taking place one after another, the online game is not just an online game any longer.

However, the "security requirements" and "virtual property protections" for online gaming seem to attract little attention from vendors and the public. More and more ways of cheating along with the accompanying criminal behaviors have been struck against our society and the computer gaming industry. Increasingly there is a strong interest in protecting the virtual properties and promoting the degree of security requirement in order to prevent the losses.

V. Prevention And Suggestion

A. *Prevent the Identity Theft*

User authentication for online gaming has mostly adopted the static password mechanism since it provided simplicity, ease and convenience. Nevertheless, it is not "up to the job" since many virtual properties are so valuable and important to users. Unfortunately, cheating programs and Trojan backdoor programs are ubiquitous throughout the Internet such that users are easily victimized through email, instant messaging and web-pages. According to our statistics, more and more criminal cases were caused by the lack of a strong authentication mechanism for online gaming. Players are eager to protect their valuable virtual property, but traditional protection mechanisms provided by vendors are no longer adequate.

In order to have simplicity, mobility, security, ease of use, convenience and low cost. It is important to combine present authentication mechanisms with practicality for online gaming. We list several popular authentication methods and compare their pros and cons as follows.

1) *Static Password:* used by most online gaming vendors and is the most convenient for players. However, the UserID and password are vulnerable. Once a Trojan horse program is hidden within the victim's computer, hackers can steal the UserID and password effortlessly and promptly.

2) *Digital Certificate:* players need to apply for certificates from a certification authority (CA) in advance. Players find the procedure complicated and the need to have the digital certificate at hand is inconvenient and affects their interest in the game.

3) *Smart Card:* also called intelligent card, needs the card reader and related software pre-installed. Most players and Internet cafés don't have card readers. In addition, it is also inconvenient for carrying their reader device.

4) *Biometric Authentication:* such as fingerprint verification, hand geometry, iris scanning, retina scanning, voice recognition, signature verification or facial recognition. These authentication mechanisms all need particular devices or readers to function. Players may feel uncomfortable and find it too complicated for everyday use.

5) *Password Transmitted via Cell Phone:* gaming authentication servers used related definitions and calculations to produce random passwords and then transmit them to players through the cell phones. Due to the prevalence of cell phones, this authentication mechanism provides a feasible, effective, and secure scheme, but cost considerations would be a big issue and cell phones are needed. Otherwise, unless the message has appropriately encrypted, cellular transmissions could be intercepted, or this method is still taking risk.

6) *Dynamic Password Authentication:* known as One-time Password Generators; this is similar to traditional static passwords since a password is used in conjunction with a UserID. However, they are limited to one time use [29]. The advantage of this technique is preventing the replay of a compromised password. Often, one-time passwords are used not only in conjunction with UserIDs but also with other passwords or PINs (Personal Identification Numbers). Commonly, a small hand-held device, which is smaller than the size of a credit card, synchronizes with the target system's authentication scheme and displays a one-time password that periodically changes (e.g., every minute). To access the target system, the user enters an assigned UserID and Password followed by the one-time password currently displayed on the hand-held device. This method of authentication provides high security, portability and low cost, since the user must possess the UserID and password as well as the authentication one-time password. If the device is lost, the user can cancel the UserID immediately. Other people have no way to find out how to use this device. Therefore, it is the most feasible solution.

In the following Table I, we compare with six authentication methods against simplicity, mobility, security, ease of use, convenience, and cost.

TABLE I.
THE COMPARISON OF SIX AUTHENTICATION MECHANISMS

	Simplicity	**Mobility**	**Security**	**Ease of Use**	**Convenience**	**Cost**
1. Static Password	High	High	Low	High	High	Low
2. Digital Certificate	Low	Medium	High	Low	Low	Medium
3. Smart Card	Medium	High	High	Low	Medium	Medium
4. Biometric Authentication	Low	Medium	High	Medium	Medium	High
5. Password Transmitted via Cell Phone	High	High	Medium	High	High	High
6. Dynamic Password Authentication	High	High	High	High	High	Medium

B. *Other Prevention and Suggestion*

According to the above analysis and statistics of online gaming crime, we give the following additional protective measure and suggestions.

1) Enhance the identity authentication mechanisms of your online gaming system by, for instance, using dynamic password authentication or a strong advanced method to protect players.
2) Use insurance to protect virtual property.
3) Register the user's identity in environments such as Internet café as far as possible. Internet Cafés and other public places providing should record their customers' identities, time period of online use, and other data to support of the investigation of criminal activities.
4) Deploy the built-in cheating detection mechanism.
5) Record complete audit data and reserve it at least three months. The online gaming vendors need to enhance itself auditing system, record and store important information like virtual property transferred record, etc. for tracing or investigating of enforcement authority.
6) Provide online scanning when players launch their gaming system. The online gaming software should provide online scan mechanisms to detect Trojan horse programs, viruses, worms, or other malicious software, which may compromise UserIDs and passwords or damage a user's system.
7) Improve related legal education. According our statistics, there are more than 71% of offenders were under 20 years old. In this age bracket, people easily breach the law and lack legal or moral education. Teachers and parents should learn and understand the negative influence of online gaming on their students or children.

8) Educate players to keep their UserIDs and passwords secret, and let them know that this is their responsibility.
9) Establish safe trading schemes or channels. Players should be very careful during online trading. Exchanging, selling, or purchasing virtual properties via a trusted third party can provide a safer environment than trading in private.
10) Assemble the related work such as legislation, standards investigation, skills for detection and tracing for use by enforcement authorities.

VI. CONCLUSION

Along with the success of online gaming, the negative influences of online gaming have become a serious issue to our teenagers and society. It not only leads to addition but also causes a number of criminal problems. Though the criminal problems are not as serious as conventional violent crimes, people still need to be aware of the problems arising from online gaming. Online gaming is one of those areas where domain specialists are not security experts, and security specialists are not familiar with complicated domain knowledge that may appear to be easy. Little serious security research has been done, though many interesting security challenges are there. It is clear that implementing measures to mitigate crime is necessary. Entertainment should return to entertainment, and not become criminal or social issues. In addition to pursuing profits, the gaming vendor needs to think and acts like an educator. We expect that these online gaming issues can come to public awareness and be solved through education, laws and technologies.

REFERENCES

[1] Global online games, Datamonitor Corp., November, 2002
[2] Earnings Release 4Q, 2003, NCsoft Corp., February 12, 2004
[3] Analysis of Taiwan's online gaming industry, Taiwan Gamania Corp., August, 2003
[4] Yahoo Corp., Http://auctions.shopping.yahoo.com/
[5] Ultima Online, Electronic Arts Corp., Available: http://www.ea.com
[6] Everquest Online, SONY Corp., Available: http://www.sony.com
[7] Matt Kiefaber, Implications of online gaming, Accessed June 20, 2004, http://www.units.muohio.edu/psybersite/cyberspace/onlinegames/index.shtml
[8] Mark D. Griffiths, Mark N.O.Davies, Breaking the stereotype: the case of online gaming, Cyber Psychology & Behavior, Volume 6, Number 1, 2003
[9] Lineage 2 Kain Lvl 57Silver Ranger, Accessed June 20, 2004, http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&item=8113549502&indexURL=0&photoDisplayType=2#ebayphotohosting
[10] Itembay Taiwan Corp., Available: http://www.itembay.com.tw, Accessed June 20, 2004
[11] A virtual dragon-sky knife is sold on $4800 U.S. dollars in charity bazaar, United Daily, Taiwan, January 29, 2003
[12] Diablo, Blizzard Entertainment Corp., Available: http://www.blizzard.com/diablo/
[13] Lineage II 2 US kain Server custom 50 level char, Accessed June 20, 2004, Available: http://cgi.ebay.com/ws/eBayISAPI.dll?ViewItem&category=4596&item=8112795841&rd=1
[14] Annual criminal statistics report, National Police Administration, Taiwan, 2003
[15] Kunt Hakon T. Morch, Cheating in online games – Threats and solution Version 1.0, Norsk Regnesentral Corp., January 8, 2003, P4
[16] Jin-Yong Online, Chinesegamer International Corp, Available: http://jy.chinesegamer.net/
[17] Three Kingdoms Online, Chinesegamer International Corp., Available: http://sy.chinesegamer.net/
[18] MU Online, Instant Reaction Corp., Available: http://www.insrea.com.tw/main.html
[19] CrossGate Online, Softstar Corp., Available: http://cg.joypark.com.tw/
[20] FreeWG Corp., Available: http://www.freewg.com/sort/1_1.htm
[21] H. Chen, Fifty thousand online gaming criminal cases happened in one year, United Daily, Taiwan, April 23, 2002
[22] Chen Kun Fu, A girl was cheated US$ 42,000 dollars via online trading, United Daily, Taiwan, February, 25, 2004
[23] Hankyoreh, Online cheating is ubiquitous, May 9, 2001, Available: http://www.hani.co.kr,
[24] Proclamation of a cheating program maker, June 27, 2004, Available: http://uvl3.24cc.cc/
[25] Chen Kun Fu, The virtual property of twenty players were stolen, United Daily, Taiwan, November 21, 2003
[26] Kidnapped for the Lineage's virtual money, United Daily, Taiwan, March 7, 2002
[27] Upset to be killed in the game, loser beaten up winner, Liberty Times, Taiwan, March 19, 2002
[28] Inside thief stealing Lineage virtual property in game company, United Daily, Taiwan, February 28, 2002
[29] Best Practices - User Authentication Mechanisms, Available: http://www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/Authentic.htm#Dynamic
[30] Dynamic password identification device manufactured by Hasng-kang Technologies, Available: http://security.fast.com.tw/product/

Ying-Chieh Chen is a National Science Council, Taiwan Scholar working as a guest worker in the Information Security Group of Institute of Information Technology, National Research Council, Canada, where he is collaborating on information security research until January 2005. He is also a Ph.D. Candidate in the Information Management Department at the National Chiao-Tung University (NCTU), Taiwan. Since 1997, he has also been police officer as cybercrime investigator in Taipei County Police Bureau, Taiwan, where he works as the manager of the cybercrime unit.

Patrick S. Chen now is a professor and he is also the Director of the Department of Information Management, Central Police University, Taiwan. He obtained his doctor degree in informatics from RWTH Aachen, Germany. He has served as an engineer in companies and a lecturer in colleges. He has published many papers and his research interests include computer crime, information systems, operations research, and electronic commerce.

Ronggong Song received his B.Sc degree in mathematics in 1992, M.Eng degree in computer science in 1996, Ph.D. in network security from Beijing University of Posts and Telecommunications in 1999. He had employed as Network Planning Engineer at Telecommunication Planning Research Institute of MII, P.R.China, and Postdoctoral Fellow at University of Ottawa, Canada. Now, he is working as a research officer at National Research Council of Canada. His research interests are privacy protection, network security, e-commerce and IP mobility.

Larry Korba is the group leader of the Information Security Group of the National Research Council of Canada in the Institute for Information Technology. He is currently involved in several projects related to security and privacy. His research interests include privacy protection, network security, and computer supported collaborative work.