An analysis of online gaming crime characteristics

Ying-Chieh Chen
Institute of Information Management, National Chiao-Tung University, Taipei, Taiwan, Republic of China

Patrick S. Chen
Institute of Information Management, Tatung University, Taipei, Taiwan, Republic of China

Jing-Jang Hwang
Institute of Information Management, Chang-Gung University, Taipei, Taiwan, Republic of China, and

Larry Korba, Ronggong Song and George Yee
Institute for Information Technology, National Research Council Canada, Ottawa, Canada

Abstract

Purpose – To arouse the public awareness of online gaming-related crimes and other societal influences so that these problems can be solved through education, laws and appropriate technologies.

Design/methodology/approach – A total of 613 criminal cases of online gaming crimes that happened in Taiwan during 2002 were gathered and analyzed. They were analyzed for special features then focusing on the tendency for online gaming crime. Related prosecutions, offenders, victims, criminal methods, and so on, were analyzed.

Findings – According to our analysis of online gaming characteristics in Taiwan, the majority of online gaming crime is theft (73.7 percent) and fraud (20.2 percent). The crime scene is mainly in internet cafés (54.8 percent). Most crimes are committed within the 12:00 to 14:00 time period (11.9 percent). Identity theft (43.4 percent) and social engineering (43.9 percent) are the major criminal means. The offenders (95.8 percent) and victims (87.8 percent) are mainly male and offenders always proceed alone (88.3 percent). The age of offenders is quite low (63.3 percent in the age range of 15-20), and 8.3 percent of offenders are under 15 years old. The offenders are mostly students (46.7 percent) and the unemployed (24 percent), most of them (81.9 percent) not having criminal records. The type of game giving rise to most of the criminal cases is Lineage Online (93.3 percent). The average value of the online gaming loss is about US$459 and 34.3 percent of criminal loss is between $100 and $300.

Research limitations/implications – These criminal cases were retrieved from Taiwan in 2002. Some criminal behavior may have been limited to a certain area or a certain period.

Practical implications – Provides a useful source of information and constructive advice for the public who will sense the seriousness and influence of online gaming crimes. Further, this topic may have implications on e-commence, e-services, or web-based activities beyond gaming.

Originality/value – Since there is little published research in this area, this paper provides the public with a good and original introduction to a topic of growing importance.

Keywords Video games, Internet, Crimes, Online operations, Taiwan

Paper type Research paper

Internet Research
Vol. 15 No. 3, 2005
pp. 246-261
Emerald Group Publishing Limited
1066-2243
DOI 10.1108/10662240510602672

1. Introduction

The development of information, software application and network technology has seen prosperous growth in recent years. In this technology development, the online multiplayer gaming has become a very successful industry and become a leader in entertainment in the world. This novel application combines multimedia, 3D, artificial intelligence, broadband networks, sound effects, computer interaction and so on, and has evolved into a highly popular form of entertainment, touching many households such as computer-based online games, Microsoft's Xbox, Sony's PS2, etc. It not only rapidly accumulates adherents but also involves diverse and interactive appeal.

Within various online games, massively multiplayer online role-playing games (MMORPGs) are currently the most successful applications, especially in Asia and North America. An MMORPG is a form of computer entertainment played by one or more persons over the internet. Through interaction and accumulation of virtual property with MMORPGs, people gain more pleasures and profits than from other traditional games.

To avoid the piracy problem often found with other types of software, many online gaming vendors in Asia have adopted the "charge for network connection" business model instead of "charge for software license" (Chen *et al.*, 2004). In a MMORPG series, players have to pay a network connection fee for operating their virtual character, while playing the game and collecting virtual properties. Since the number of virtual properties (like virtual sword, helmet or equipment) is limited and some virtual equipment cost money, time and energy to develop, a market has emerged for them. Some players who need or desire certain equipment trade for them. In fact, some virtual properties have very high monetary values in the marketplace. Even the virtual currency in an online game can be converted into cash through exchange with other players. Take "Lineage Online" for example, the virtual currency exchange rate was 2,500:1 (2,500 virtual currency can be converted to US$1) in August 2002 and 10,000:1 in March 2003. These facts indicate that virtual property trading is indeed flourishing.

Unfortunately, with the growth of online gaming, there has been an amazing growth in the online gaming-related crimes (offenders are mostly in the age range of 15-20), particularly in MMORPG games. Such cyber-criminal activity within online games is increasing at an alarming rate. In 2002, the number of thefts, fraudulent activities, robberies, counterfeited documents, assault and batteries, threats and illegal gambling cases from online games increased to 1,300 from 55 only two years earlier; furthermore, online gaming-related crime has become the most serious problem within all cyber-criminal cases in Taiwan (Chen *et al.*, 2004).

In our previous research, we illustrated the online gaming crime and security problems (Chen *et al.*, 2004), analyzed the influence of online gaming crime (Chen *et al.*, 2003), and gave a classification for a variety of criminal behaviors (Chen *et al.*, 2005). Since there is little published research in this area, in this paper we gather 613 criminal cases from Taiwan related to the online gaming crime, and analyze them for:

- reasons for prosecution;
- offender's gender and age range;
- criminal method;
- crime scene;
- time;
- the market value of virtual property for each case, and so on.

The sources for this research are Taiwan's judicial documents that are retrieved for the purpose of research under privacy protection agreements. This paper is intended to provide a thorough illustration of online gaming crimes and security problems as well as some present possible countermeasures.

The remainder of this paper is organized as follows. In Section 2, we define online gaming, online gaming crime, and MMORPG. In Section 3, we analyze the statistics of online gaming crime along with the criminal cases themselves. To further describe the criminal behavior and tendency, we categorize the approaches used in the commission of these crimes in Section 4. In Section 5, we present possible suggestions and methods of prevention to solve these problems. We give our conclusions in Section 6.

2. Definition

In this section, we illustrate the definition of online gaming, online gaming crime, and MMORPG.

2.1 Online gaming

Online gaming or online games are the games that are played online via a local area network (LAN), internet, or other telecommunication medium. They are distinct from video or computer games that are not networked. Normally, the technical requirement for playing online games is a web browser and/or appropriate client software and a network connection. A game played in a browser is called a browser-based game or a web game. Online gaming includes MMORPG gaming, internet gaming, web gaming, online gambling, local LAN gaming, and mobile gaming, but not the non-networked video and personal computer gaming. The MMORPG, internet, web and online gambling games are generally operated through a wide-area/public network environment. Figure 1 gives a map of the online gaming landscape.

2.2 Online gaming crime

Online gaming crime comprises a criminal activity in which an individual, a computer, and a network game are the key entities involved. Some online gamers use illegal or immoral means to gain advantage in their online games. Exactly which of these means

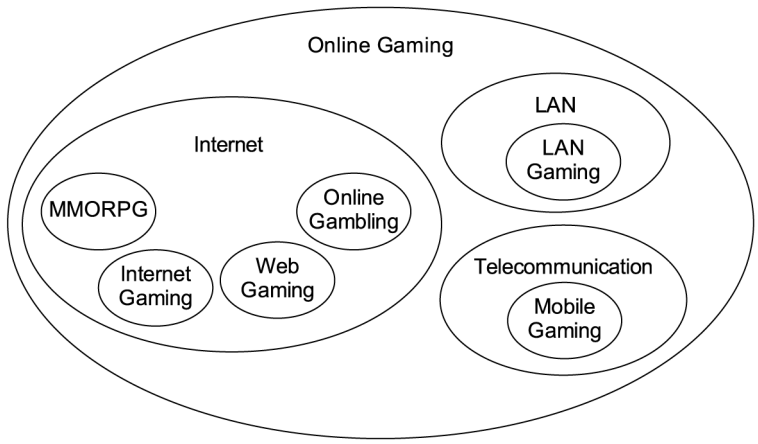


Figure 1.
Classification of online games related to communication medium

is illegal varies greatly by province/state, territory, and country. Examples of online gaming crime are:

- theft;
- fraud;
- robbery;
- kidnapping;
- threat;
- assault and battery;
- destruction of property;
- counterfeiting;
- receipt of stolen property
- privacy violations;
- software piracy;
- extortion;
- gambling, and so on.

Table I depicts the detailed classification of online gaming crimes and crime types (Yan and Choi, 2002; Chen *et al.*, 2004). Most of the cases can be attributed to theft and fraud; nevertheless, we list some of the possible derivative crimes.

2.3 MMORPG

MMORPGs belong to one of the online gaming categories. We can trace its roots to non-graphical online Multi-User Dungeon games (MUD). These include text-based computer games such as Adventure and Zork, and pen and paper role-playing games like Dungeons & Dragons. Most MMORPGs are commercial in that a user must pay money for the client software and/or a network connection fee to play. Yet there are some totally free-of-charge MMORPGs that may be found on the internet, although their quality is generally lower compared to commercial ones.

Some of the current popular commercial MMORPGs are Ultima Online (1997), Lineage (1998), EverQuest (1999), Dark Age of Camelot (2001), Star Wars Galaxies (2003), and Final Fantasy XI (2003). Of all MMORPGs, Lineage has the most subscribers and is the most popular in South Korea and Taiwan.

There are also several projects in development to create high-quality free MMORPGs, such as PlaneShift, or a free game engine for MMORPGs, such as Arianne (*Wikipedia Online Encyclopaedia*, 2004).

3. Statistics of online gaming crimes

We randomly chose 613 online gaming criminal cases as examples. The cases occurred during 2002 in Taiwan. These criminal cases are from official crime reports, from different judicial or investigative authorities. The majority (427 cases or 69.7 percent) of the 613 cases are from the local branch of investigative authority and the remainder are from the professional cybercrime unit. We will analyze them for special features focusing on the tendency for online gaming crime, examining related prosecutions, offenders, victims, and criminal methods. Regarding the criminal cases, we divided

I. Theft	Theft of UserID and password (or identity)
	Theft of virtual property
	Theft of Monthly Game Card
II. Fraud	Fraud by trade or exchange
	Fraud by identity
	Fraud by alliance
	Fraud by collusion
	Cheating the online gaming vendor
	Fraud by abusing policy
	Cheating related with virtual property
	Fraud by compromising password
	Fraud by sharing UserID and password
	Fraud by denying service to peer players
	Fraud due to lack of secrecy
	Fraud due to lack of authentication
	Fraud-related internal misuse
	Fraud by social engineering
	Fraud by modifying game software or data
	Fraud by exploiting bugs or design flaws
	Fraud by faking official web site
III. Derivative crimes	Robbery
	Kidnapping
	Threat
	Assault and battery
	Destruction of property
	Counterfeit of property
	Reception of stolen property
	Privacy violations
	Software piracy
	Extortion
	Gambling

Table I.
Classification of online gaming crimes

them into four categories, such as identity theft, social engineering, hacking tools or system weakness, and force or revenge. To clarify the term on identity theft and social engineering, a brief definition is given as follows:

(1) *Identity theft*. Identity theft is a term used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain (US Department of Justice, 2004).

(2) *Social engineering*. In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures (SearchSecurity Corp, 2004).

3.1 Case analysis

Using the above criminal cases, we first analyze their distribution with respect to different attributes of prosecution including: type of crimes, time of occurrence, date, crime scene, and monetary value.

(1) *Type of crimes*. Theft and fraud are the major type of online gaming crimes. For example, Table II depicts that 73.7 percent of cases were charged with theft, 20.2 percent of cases were fraud.

(2) *Type of online games*. For example, Table III shows that 93.3 percent of the criminal cases happened on Lineage online game.

(3) *Time of crime distribution*. For example, Table IV and Figure 2 show that the highest rate (11.9 percent) of online gaming crime happened during the period 12:00 to 14:00.

(4) *Crime scene distribution*. For example, Table V shows that most criminal activities were committed in internet cafés (54.8 percent). In addition, many offenders also used their home network (30.8 percent) to commit the crime.

Measure	Value	Frequency	Percentage
Type of crimes	Theft	452	73.7
	Fraud	124	20.2
	Robbery	9	1.5
	Threat	2	0.3
	Others	26	4.2
Total		613	100.0

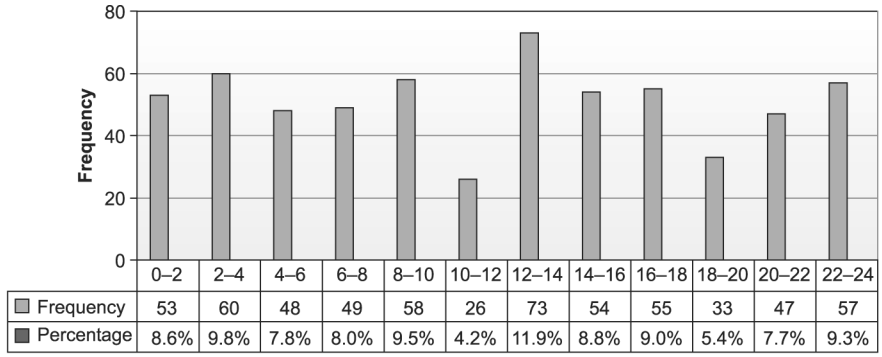
Table II. Frequency of occurrence of different types of crime

Measure	Value	Frequency	Percentage
Type of online games	Lineage	572	93.3
	JinYong online	23	3.8
	StoneAge	10	1.6
	CrossGate	3	0.5
	Others	5	0.8
Total		613	100.0

Table III. Frequency of crimes based on different online games

Measure	Value	Frequency	Percentage
Crime time	0-2	53	8.6
	2-4	60	9.8
	4-6	48	7.8
	6-8	49	8.0
	8-10	58	9.5
	10-12	26	4.2
	12-14	73	11.9
	14-16	54	8.8
	16-18	55	9.0
	18-20	33	5.4
	20-22	47	7.7
	22-24	57	9.3
Total		613	100.0

Table IV. Time of crime occurrence distribution



	0–2	2–4	4–6	6–8	8–10	10–12	12–14	14–16	16–18	18–20	20–22	22–24
Frequency	53	60	48	49	58	26	73	54	55	33	47	57
Percentage	8.6%	9.8%	7.8%	8.0%	9.5%	4.2%	11.9%	8.8%	9.0%	5.4%	7.7%	9.3%

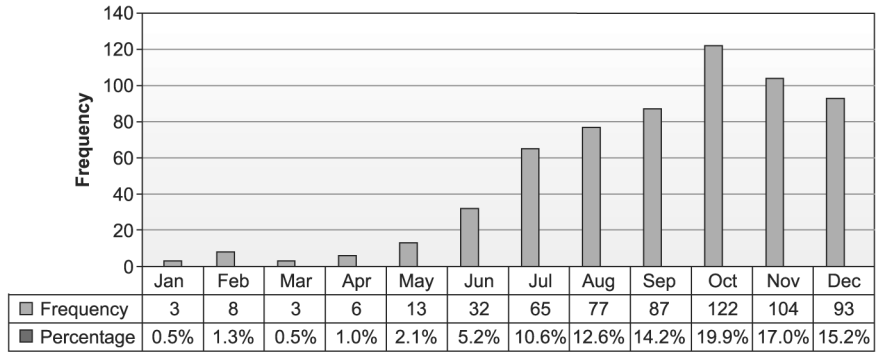
Figure 2.
Time of crime distribution

Measure	Value	Frequency	Percentage
Crime scene	Internet café	336	54.8
	Offender's dwelling	189	30.8
	Victim's dwelling	22	3.6
	School	4	0.7
	Others	62	10.1
Total		613	100.0

Table V.
Crime scene distribution

(5) *Crime date distribution*. Figure 3 shows that online gaming criminal cases have been increasing rapidly. For example, the number of cases from July to December is about 89 percent of cases in the whole year.

(6) *Market value of each case distribution*. In the 613 cases, the average value of the online gaming crime loss is about US$459, but 18.1 percent of cases have no record of the lost value. Table VI depicts the distribution of the criminal cases based on lost value.



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Frequency	3	8	3	6	13	32	65	77	87	122	104	93
Percentage	0.5%	1.3%	0.5%	1.0%	2.1%	5.2%	10.6%	12.6%	14.2%	19.9%	17.0%	15.2%

Figure 3.
Crime date distribution

Measure	Value	Frequency	Percentage
Market value of each case (US dollars)	No record	111	18.1
	<100	96	15.7
	100-300	210	34.3
	301-500	48	7.8
	501-700	54	8.8
	701-900	34	5.5
	901-1100	10	1.6
	1,101-1,300	20	3.3
	1,301-1,500	7	1.1
	>1,500	23	3.8
Total		613	100.0

Table VI. Market value of each case distribution

3.2 Offender analysis

In this section, we analyze the distribution of online gaming crime cases based on the different attributes of offenders, including offender's gender, age, profession, whether the offender had a criminal record, and whether the offender colluded with others:

(1) *Gender*. Table VII shows that within 613 cases, there are 587 male offenders, which is 95.8 percent of the whole offenders. The number of female criminals is 26, which is 4.2 percent of the offenders.

(2) *Age*. Table VIII shows that young offenders between 15 and 20 years old have the highest number of offenders (63.3 percent).

(3) *Profession*. Table IX shows that most of the offenders are students. The main professions of the offenders include students, workers, military, and SOHO. The unemployed make-up one-fourth of all offenders.

(4) *Having criminal record*. Table X indicates that 18.1 percent of offenders had committed prior crimes.

Measure	Value	Frequency	Percentage
Gender	Male	587	95.8
	Female	26	4.2
Total		613	100.0

Table VII. Offender's gender distribution

Measure	Value	Frequency	Percentage
Age	<14	52	8.5
	15-20	388	63.3
	21-25	135	22.0
	25-30	26	4.2
	31-35	10	1.6
	36-40	0	0.0
	>40	2	0.3
Total		613	100.0

Table VIII. Offender's age distribution

Measure	Value	Frequency	Percentage
Profession	Student	286	46.7
	Unemployed	147	24.0
	Worker	78	12.7
	Military	44	7.2
	SOHO	31	5.1
	Business	9	1.5
	IT	2	0.3
	Medical	1	0.2
	Others	15	2.4
Total		613	100.0

Table IX.
Distribution of offender's profession

Measure	Value	Frequency	Percentage
Have criminal record?	Yes	111	18.1
	No	502	81.9
Total		613	100.0

Table X.
Having criminal record distribution

(5) *Colluding with others*. Table XI shows that 11.7 percent of offenders colluded with others.

3.3 Victim analysis

In this section, we analyze the distribution of the online gaming crime cases with respect to different victim attributes, including victim gender, age range, and profession:

(1) *Gender*. Compared to the offender's gender distribution, the percentage of male victims is less than the percentage of male offenders but the percentage of male victims is much more than the female victims. Table XII shows that there are 538 male victims that is 87.8 percent of the cases.

(2) *Age*. In Table XIII, young victims between 15 and 20 years old were involved in the highest number of cases (41.3 percent). However, this is still lower than for

Measure	Value	Frequency	Percentage
Collude with others?	Yes	72	11.7
	No	541	88.3
Total		613	100.0

Table XI.
Distribution of collusion

Measure	Value	Frequency	Percentage
Gender	Male	538	87.8
	Female	75	12.2
Total		613	100.0

Table XII.
Victim's gender distribution

the corresponding age group of offenders (Table VIII). This is balanced by the fact that victims between 21 and 25 have a higher number of cases than the corresponding age group of offenders (Table VIII).

(3) *Profession*. Table XIV shows the distribution of the victims with respect to professions. Compared to the criminal profession distribution, the number of cases of the victim students is considerably fewer than those for the offender students, but they still represent the largest number of cases over all victims. The main professions of the victims are still students, the unemployed, workers, military, SOHO, and business. The unemployed represent one-fifth of all victims.

3.4 Criminal method analysis

In order to analyze online gaming crime, we categorize the 18 criminal methods into four categories, which are identity theft, social engineering, hacking tools or system weakness, and force or revenge. Table XV depicts the detailed criminal methods with corresponding number of criminal cases and percentages. We bypassed 247 cases from our official report that had no mention of the exact criminal methods used. Figure 4 gives a pie chart of these four categories of online gaming crime.

4. Criminal behavior analysis and trend

4.1 MMORPGs being attractive to players and criminals

There are a number of reasons why MMORPGs are attractive to both players and criminals alike. These reasons include:

Measure	Value	Frequency	Percentage
Age	<14	21	3.4
	15-20	253	41.3
	21-25	205	33.4
	25-30	91	14.8
	31-35	26	4.2
	36-40	9	1.5
	>40	8	1.3
Total		613	100.0

Table XIII.
Victim's age distribution

Measure	Value	Frequency	Percentage
Profession	Student	209	34.1
	Unemployed	132	21.5
	Worker	100	16.3
	Military	35	5.7
	SOHO	41	6.7
	Business	41	6.7
	IT	7	1.1
	Others	48	7.8
Total		613	100.0

Table XIV.
Professional distribution of victims

Criminal methods	Frequency	Percentage
I. Identity theft		
Exploit sharing UserID and password	54	14.75
Exploit observing other players' UserID and password	42	11.48
Steal others' UserID and password	51	13.93
Exploit sharing virtual properties with others	8	2.19
Exploit victim's carelessness	4	1.09
Subtotal	159	43.44
II. Social engineering		
Cheat on identity	52	14.21
Cheat on trade or exchange	46	12.57
Cheat on virtual property	24	6.56
Cheat on sharing UserID and password	11	3.01
Other social engineering means	11	3.01
Cheat to online gaming vendor	9	2.46
Cheat on alliance	8	2.19
Subtotal	161	43.99
III. Hacking tools or system weakness		
Exploit Trojan or other hacking tools	32	8.74
Compromise password	8	2.19
Exploit weakness of gaming software or system	2	0.55
Exploit internal abuse of vendor	1	0.27
Subtotal	43	11.75
IV. Force or revenge		
Use force to get UserID and password	2	0.55
Revenge in real life	1	0.27
Subtotal	3	0.82
Total	366	100.00

Table XV.
Criminal method distribution

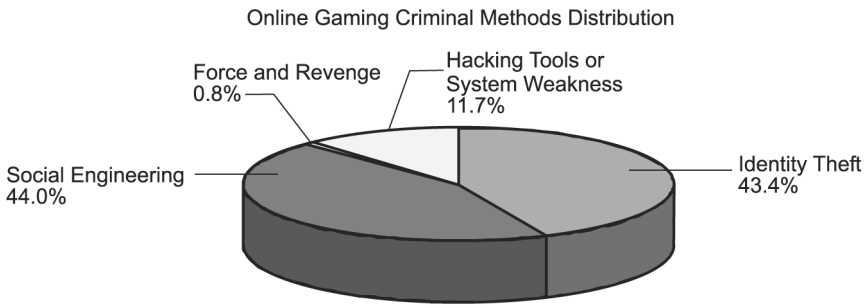


Figure 4.
The pie chart of the four criminal method categories

- many MMORPGs provide a very good challenge and also there is a large community of players;
- players and criminals desire to gain rare virtual property or virtual money;
- players can accumulate virtual fortune gradually and in the cases of some games, it can be converted into cash;

- many MMORPGs represent great amusement;
- there is a challenge in moving their virtual character to a higher level;
- criminals find that the lack of authentication/security schemes makes it easy to profit by illegal means;
- some virtual properties are highly valuable in marketplace;
- there is a market for virtual property trading because sufficient numbers of people would rather pay money for virtual property rather than the energy, skill, or time to work within the game;
- the trade and exchange of virtual property has become prevalent;
- the perception of MMORPGs has changed to the point where many people now think they are making money instead of just for entertainment; and
- it is apparent that the different business model for MMORPGs in Asia (as opposed to North America) leads to higher MMORPG crime rate (Chen *et al.*, 2004).

4.2 Criminal behavior analysis

We first analyze the main reasons for some online gaming crimes, and then summarize a variety of criminal behaviors. As we have described, 93.3 percent of criminal cases happened within the Lineage online game. We give the following analysis:

- Lineage is the earliest and biggest online game in terms of market scale. During 2002, it claimed over 2.5 million memberships in Taiwan.
- Many virtual properties in Lineage have a higher value in the real market than other games.
- Gamania Corp., the source of Lineage, provides more detailed log record information with which investigators can easily trace criminal footprints as evidence. Thus, information on Lineage criminal activity is more complete, leading to more criminal cases identified with Lineage. On the other hand, most other vendors lack adequate audit schemes or cooperative strategies with enforcement authorities. Therefore, for these vendors, the enforcement authorities could not execute their investigations or were prohibited by limited evidence.

From the criminal methods study, it was shown that exploiting shared UserID to which more than one player uses the same UserID and password has the highest criminal rate of about 14.7 percent. This means exchanging UserID among players becomes common, but this easily leads to possible offenses such as virtual property theft or fraud, etc. In addition, since the UserID and password provide access to everything owned by players in the virtual world, most criminal cases are related to identity theft (43.4 percent). These cases include:

- exploiting shared UserID and password;
- covertly observing other player's UserID and password;
- exploiting shared virtual properties with others;
- exploiting the victim's carelessness;

- use of Trojan backdoor programs; and
- related illegal means to gain others' UserID and password.

Different online gaming vendors may have different administrative mechanisms; for instance, some vendors can record and audit details regarding virtual property trading, transference, dropping, processing, etc. but others may only record little information about logon and/or logoff. Once a dispute happens, it may be difficult to distinguish who is right or wrong. If a vendor were lacking a scheme for auditing and tracing of record information, it would lead to problems in carrying out prosecution.

4.3 Online gaming crime trends

From the statistics and our consequent analysis, we find that online gaming crime has the following trends:

- Online gaming crime is growing rapidly. From the statistics, the cases that happened in the second half of the year were 89.4 percent of the cases for the whole year.
- The age of the online gaming offenders is going down. From the statistics, the online gaming offenders between 15 and 25 years old were 85.3 percent of all offenders. The young offenders under 14 years old were 8.5 percent of all offenders.
- Males exhibited more criminal behaviors. The statistics show that males comprised 95 percent of all offenders.
- The internet café has been the main crime scene.
- Students and the unemployed were the main online gaming offenders, with a rate of 46.7 percent for students and 24 percent for the unemployed.

5. Suggestions and crime preventions

In this section, we suggest potential approaches for dealing with the rising incidence of gaming crime.

5.1 Preventing identity theft

Identity theft is a key problem area. Some approaches to preventing criminal activity in this area include:

(1) *Use of virus and Trojan scanning software*. For instance, the online gaming service provider could run this as part of its operation for all client software.

(2) *Online tests of the username password efficacy*. At enrollment, the online gaming service would check the effectiveness of a selected username and password.

(3) *Requiring changes of username/password*. Every few weeks the gaming service would require the user to change the username/password to new ones.

(4) *Detection of suspicious activity*. The online gaming service would detect when there is more than one instance of a supposedly unique player being online in order to detect sharing of username/password.

(5) *Use of digital certificates*. Players would be required to apply for certificates from a certification authority (CA) in advance. Unfortunately, players may find this procedure complicated. The need to have the digital certificate at hand is

considered inconvenient, may hamper mobility and thus would affect the players' interest in the game.

(6) *Smart card to identify users*. While effective for authenticating users, it unfortunately adds to the cost of the game, and would require a card reader.

(7) *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 them too complicated for everyday use.

(8) *Password transmitted via cellphone*. Gaming authentication servers use related definitions and calculations to produce random passwords and then transmit them to players through cellphones. Owing to the prevalence of cellphones, this authentication mechanism could provide an effective and secure scheme, but cost considerations would be a big issue. Also, players must have cellphones. Furthermore, unless the message has been appropriately encrypted, cellular transmissions could be intercepted.

(9) *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. They are limited to one-time use (Information Technology Support Center, 2004). The advantage of this technique is preventing the replay of a compromised password.

5.2 Other protective measures

Other protective measures include the following:

- Use insurance to protect virtual property. While not preventing the crime, it would compensate for loss. Systemically, insurers may require online gaming service providers to maintain certain security standards.
- Deploy built-in cheating detection mechanisms. The major objective for this measure is to reduce the modification of game software and use of fraudulent means so as to shrink the possibility of criminal activities. Such a system would detect or discover unusual activities or modifications, and produce related alarms. Some online gaming vendors, such as Joe Wilcox, have developed similar mechanisms (Unreal Playground, 2002).
- Advise the vendor's customers exactly what information the vendor will, and will not ask for on web sites or via email. If personal, financial or sensitive information must be exchanged, the vendor must clearly indicate under what conditions that exchange will occur.
- Build-up an instant response/report platform. Using this platform, vendors can instantly provide essential information or case study with their customers on investigating or reporting suspicious/illegal means or circumstances. Effectively this would be a call centre focused on dealing with potentially illegal behavior.
- Be the first to establish similar web site domain URLs. For example, www.googel.com will still take users to the proper web address, www.google.com. The idea behind this is to help prevent fake web sites.

- Register the user's identity in environments such as, internet cafés as far as possible. Internet cafés and other public places providing online gaming should record their customers' identities, time period of online use, and other data to support the investigation of criminal activities.
- Record complete audit data and keep it at least three months. Online gaming vendors need to enhance their auditing systems, as well as record and store important information such as a record of virtual property transferred, for tracing or investigating by an enforcement authority.
- Improve related legal education. According to our statistics, more than 71 percent 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.
- Educate players to keep their UserIDs and passwords secret, and let them know that this is their responsibility.
- 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.
- Deploy rights management mechanisms to lock virtual property for use by only those authorized.
- Law enforcement authorities can employ "honey pots" to lure and capture online gaming offenders; online gaming honey pots are fake online gaming systems that act as decoys to collect data on criminal activity (Martin, 2001).

6. Conclusion

In this paper, we gathered and analyzed 613 criminal cases of online gaming crimes that happened in Taiwan during 2002. We can imagine that the upcoming online gaming crimes and cheating cases will undermine the development of the online gaming industry. Furthermore, these crimes not only influence the players' mental addiction but also may lead to other societal problems.

Although these crime problems may not be as serious as conventional violent crimes, people need to be aware of the problems arising from online gaming, especially since the age of online gaming offenders is going down. Entertainment should be entertainment, and not become a dark corner of the internet corrupted with criminal issues.

In addition to pursuing profits, the vendors need to be educators and to a certain respect, enforcers of appropriate behavior in the playing of these online games. We hope that the online gaming related issues identified here would be noticed by our society so that these problems may be solved through education, laws and appropriate technologies. It is clear that implementing measures to mitigate crime is necessary.

In this paper, we have also provided some suggestions and preventative approaches to help deal with the criminal activity.

References

Chen, Y.C., Lin, S.K. and Hwang, J.J. (2003), "The influence of computer crime in online gaming on E-society – taking example for Taiwan in 2002", paper presented at the International Conference on Innovative Information Technology Policy and E-Society, NCCU, Taiwan.

Chen, Y.C., Chen, P.S., Song, R. and Korba, L. (2004), "Online gaming crime and security issues – cases and countermeasures from Taiwan", paper presented at the 2nd Annual Conference on Privacy, Security and Trust, Fredericton.

Chen, Y.C., Chen, P.S., Song, R., Yee, G. and Korba, L. (2005), "Classification of online gaming crime and security", paper presented at the 2005 IRMA International Conference, San Diego, CA.

Information Technology Support Center (2004), "Best practices – user authentication mechanisms", available at: www.itsc.state.md.us/oldsite/info/InternetSecurity/BestPractices/Authentic.htm

Martin, W. (2001), "Honey pots and honey nets – security through deception", available at: www.sans.org/rr/papers/4/41.pdf

SearchSecurity Corp (2004), "Definition of social engineering", available at: searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html

Unreal Playground (2002), "Exclusive interview with Dr Sin of Epic Games", available at: www.unrealplayground.com/interview.php?id = 1

US Department of Justice (2004), "Identity theft and fraud", available at: www.usdoj.gov/criminal/fraud/idtheft.html

Wikipedia Online Encyclopaedia (2004), "Definition of MMORPG", available at: en.wikipedia.org/wiki/MMORPG

Yan, J.J. and Choi, H.J. (2002), "Security issues in online games", *The Electronic Library*, Vol. 20 No. 2, pp. 125-33.