Appl. Math. Inf. Sci. 6 No. 1S pp. 291S-302S (2012)

Applied Mathematics & Information Sciences
An International Journal

An automatic and proactive identity theft detection model in MMORPGs

Jiyoung Woo[1], Hwa Jae Choi[2], and Huy Kang Kim[3*1]
[1]Graduate School of Information Security, Korea University, Seoul, Rep. of Korea
Email Address: jywoo@korea.ac.kr
[2]Graduate School of Information Security, Korea University, Seoul, Rep. of Korea
Email Address:chj870809@korea.ac.kr
[3]Graduate School of Information Security, Korea University, Seoul, Rep. of Korea
Email Address: cenda@korea.ac.kr

Received: Received May 02, 2011; Revised July 25, 2011; Accepted September 12, 2011
Published online: 1 January 2012

Abstract: Identity theft happens frequently, especially in popular multiplayer games where cyber-assets can be monetized. In this work, we propose an automatic and proactive identity theft detection model in online games. We specify the identity theft process into exploration, monetization, and theft and pose identity theft detection as a multi-class classification problem. We propose an automatic and proactive detection model utilizing rich features, along with appropriate problem-specific domain knowledge regarding the unique properties of identity theft. The proposed model based on process specification and automatic learning will reduce financial losses to game users and game companies through early detection.

Keywords: Identity theft detection, multi-class classification, online game security, MMORPG

1 Introduction

Online games have many security issues today [5, 22]. As the online game market grows and the boundary of the virtual and real economies blurs, illegal activities in online games have drastically increased and diversified. In the past, protecting information technology assets such as systems, networks, databases and applications was the priority task to enhance information security for online game companies. Today, securing the personal information and cyber-assets of online game users from cheating and hacking has become a major issue in the online game industry. We summarized the illegal activities that happen frequently in online games in table.1.

Major security problems that significantly affect game users originate from gold farming with game bots, private servers, and identity theft. While gold farming, private servers, and system/network penetration are illegal activities against the online game company, the identity theft is against game players. Identity theft, stealing identities for fraudulent use, happens frequently, especially in online multi-player games where cyber-assets can be monetized. Hackers steal items and game money from victims and monetize them into real currency. Identity theft has drawn relatively less attention from the game industry and researchers since identity theft has less influence on the entire

[1] **Corresponding Author: Huy Kang Kim, cenda@korea.ac.kr**

system/network or incurs less financial losses to online game companies than other illegal activities. However, as the factory size team (so called, Game workspace) becomes involved in virtual crimes of online games, identity theft is no longer minor issue limited to a few users. Identity theft often happens through systematic organization in a game workspace. The detection of identity theft is important to detect the huge dark organization that threatens online game companies and their users. Moreover, user IDs and passwords can be used to hack other web sites such as banking sites and may cause secondary economic losses if users use same IDs and passwords in other web sites. In a narrow view, identity theft may cause disputes between online game companies and the user and finally user's churn

Category	*Target*	*Threat description*	*Characteristics*
Gold farming	Company	Gold farming is aims to gaining cyber money from online games by running game bots at game workspace	- Game bot is an automated program that plays games on behalf of human gamers. It has several types (e.g. software, USB and mouse) - Game bots destroy the in-game balance and increase non-BOT user's claims. - In game workspace, gold farmers run factory-size game bots to collect game items or cyber money.
Illegal copyright with Private server	Company	Game servers that illegally provide the same or modified game services	- Server which is the same as a genuine one (usually the game software is copied by system hacking or internal file leakage) - Some private servers provide more experience points and items than a genuine server to attract users.
System or network penetration	Company	Intrusion of server systems or networks of game service providers	- Remote exploit attacks directly targeted for game servers, especially database systems which contain users' in-game cyber-asset or equipment data. - Once this hacking has succeeded, hackers usually run an update query to manipulate the asset or inventory records.
Identity theft (Account theft)	Customer	Stealing game users' account information (ID and password) to gain game money	- This attack is enabled by malware and categorized as a dropper or password stealer. - Hackers login with the stolen users' account information. - They transfer the illegally gained cyber-assets or monetized currency to their accounts.

Table.1 Threats in online games

In this work, we present an identity theft detection model based on user behavior analysis. In this model, we examine hacking patterns of identity theft in online games, specify them, and perform classification tasks for each specified process. This approach enables online game companies to build up detection strategy that prevents financial damage against users and companies, reduces the user inconvenience caused by client-side and network-side security solutions

2 Related Works

2.1 Security in online games

As the online games market grows and its virtual economy affects the real economy, security has become a major issue in the game industry and has also drawn much attention from researchers. Virtual crimes in online games are addressed in many studies. Yan and Randell [36] classified cheating in online games via underlying vulnerabilities, cheating consequences, and cheating principals. Their taxonomy encompasses almost all possible cheating types. Identity theft is also included as "Compromising passwords" category in their taxonomy. Hu and Zambetta [16] proposed a taxonomy framework in terms of attributes, threats, and means for MMORPG security. They addressed the elementary sources of faults and possible paths leading to these faults from the sources, as well as countermeasures to mitigate these faults. They classified the cheating forms in online games into two categories – a generic form and an online game-specific form. Bardzell et al. [5] surveyed known security vulnerabilities in MMORPGs and compared attack vectors in terms of banking, e-Bay, and MMORPGs. Chen et al. [11] investigated cheating patterns in Taiwanese online games and proposed countermeasures against identity theft. Bono et al. [7] studied several vulnerabilities in online games. These studies enable us to understand cheating activities in online games in a holistic view.

Recent studies in online game security focus on detecting gold farming. To detect game bots, various schemes have been proposed such as user behavior-based [3, 8, 32, 37], user interaction-based [24], movement-based [19, 26], HOP (Human Observation Proofs) based [14, 21], and CAPTCHA-based [35] schemes. Among bot detection methods, user behavior, movement, and traffic-based analysis are applicable to identity theft

detection. These methods derive users' unique patterns in behaviors, movements, and traffics, so they can recognize hackers' login. However, little research has applied these methods to identity theft detection.

2.2 Identity theft detection in the web and online game

Identity theft is not just technical—it also involves economic, social, and legal issues [34]. Jamieson and Stephens [18] provided a systematic analysis and categorization of the identity theft in terms of perpetrators, channels, methods of attack, victims and organizational impacts.

Chen et al. [9] addressed the severity of identity thefts in online games through investigation on real cheating cases. As the importance of security about identity theft in online games has been emphasized, researchers have begun to propose prevention and detection methods of identity theft. Biological signatures such as facial and fingerprint recognition, and behavioral signatures such as handwriting, are proposed [17, 28] as preventative methods

Ki et al. [20] mentioned that social engineering is used for ID and password impersonation in their taxonomy of online game security. Many studies on identity theft focus on building detection model for the phishing attack, a form of the identity theft based on social engineering. The summary of previous works on the phishing attack detection is shown in [2]. Chen et al. [10] assessed the severity of phishing attacks in terms of their risk levels and the potential loss in market value. They proposed a hybrid method that incorporates the text mining and data mining on textual and financial variables and can predict the severity of the attack. Chou et al. [12] and Kirda and Kruegel [24] proposed a framework for client-side defense: a browser plug-in that examines web pages and warns the user. Web spoofing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information.

Regarding the detection method of identity theft, keyboard typing patterns and mouse movement dynamics have been used [15, 28]. Chen and Hong [8] proposed a new biometric for human identification based on user gameplay activities, especially idle periods between successive movements. Melinkov and Schonwalder [25] introduced a cybermetric pattern that identifies a user based on Internet activity. They proposed a work to identify users through the detection and analysis of characteristic network flow patterns. Pao et al. [27] proposed a general approach for user verification based on user trajectory inputs.

2.3 Data mining in security

Statistical approaches and data mining techniques that extract implicit anomaly from data have been used in computer and network security. Data mining is a powerful tool that can explore large databases quickly and efficiently. Association rule mining has been used in detecting abnormal sequences from dominant patterns [33]. Bayesian inference has been used to detect anomaly patterns in datasets. The Bayesian inference model is computationally expensive as the number of variables increases. An artificial immune system has been adopted to detect intrusion. This technique collects all the known normal cases and gives an alarm when an abnormal event occurs. When the data size is huge, however, it is more efficient to learn abnormal patterns than to learn normal patterns. Neural networks are also used to learn normal patterns and predict unusual behaviors. Even though neural networks output good performance, it is hard to apply a neural network-based detection system to industry, especially for preventing identity theft. Neural networks have black box features, i.e. their detection rules are hard to be interpreted and explained in human words. When the dispute between the user and the company happens, the company cannot provide good logical arguments for users.

Chen et al. [10] used the neural network, decision tree, and support vector machine to classify risk levels in detecting phishing emails. Ahmed et al. [3] used Naive-Bayes, KNN, Bayesian network, and decision tree to detect gold farmers in MMORPGs. Abu-Nimeh and Chen [1] adopt a SVM(support vector machine) classifier to detect spam blogs. Prasetya and Zheng [29] and Gaspareto et al. [13] adopted an artificial neural network for bot detection in MMORPGs. Kim et al. [21] formulated the bot detection task as a binary classification. They set features as event sequences happening by mouse movement and key stroking. They explored various machine learning techniques such as the decision tree, neural network, k-Nearest, and Naïve Bayesian, and concluded that the decision tree method outperformed the others.

2.4 Research gaps

From the literature review on previous studies, we identified some research gaps. Even though the importance of security in online games where the virtual economy is attached to the real economy has been emphasized, little research on prevention and

detection methods of identity theft in online games has been proposed. The studies on online game security are biased towards bot detection. Few studies attempt a machine learning approach for automatic game bot detection. Previous studies on the identity theft detection mainly focus on the client-side prevention methods and some of them attempt to build biometrics, whether biological or behavioral, to identify the individual's unique patterns. However, the biometrics studies, which are server-side detection methods, require a lot of resources to be implemented in industry because it should analyze all users' behaviors and maintain identified patterns of individual users. Rather than the approach that identifies individuals' patterns, the approach that identifies the difference between genuine user's logins and hacker's logins requires less resources, works faster, and can be applied to newly subscribed users.

In addition, there is no research that deals with the systematic specification of hacking patterns in identity theft and poses detection tasks as multi-class classification to the best of our knowledge. Most previous studies using data-mining techniques approach identity theft through a binary classification problem. And last, the limited number of studies applied their methodologies to large-scale real data provided by popular online game companies. Most researchers do not own or control a large-scale online game world, so they only study small, simulated game environments. Previous research lacks in collecting the industry data and applying their models in a real game world.

3 Identity Theft Detection Model in MMORPGs

3.1 Identity Theft in MMORPGs

Identity theft is performed in various ways. First, hackers penetrate to popular but security-vulnerable web sites and inject malicious code into them. Malicious code spreads through personal computers that lack security patches. This malicious code steals user IDs and passwords. Second, hackers may penetrate computer networks, systems, and databases of online game companies and then can obtain personal data directly. Third, brute-force attack is used for password guessing.

Online game companies try to protect users from identity theft taking different countermeasures against various identity theft methods as mentioned above. To protect users from malicious code with the purpose of stealing user IDs and passwords, the online game company adopts client-side prevention methods. To enhance the security level in the client computer, on-demand anti-virus programs, anti-keylogging software, and patch management software are mostly required to run game software safely. To prevent brute-force attacks that enumerate all candidates and check each one sequentially in the same IP for a short, the online game company limits the security challenge numbers per account/IP. When multiple login failures happen, the company can block user logins using secondary authentication tools such as a Complete Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA), Mobile One-time Password (MOTP), token-type OTP, and visual keyboards. These security solutions force game users to install security tools on their computers; however, they may sometimes cause system conflicts in client computers and eventually cause the user inconvenience.

Network-side monitoring is also adopted in application of countermeasure against the brute-force attack. Most online game companies monitor top login success IP addresses and top login failure IP addresses, after analyzing these IP addresses, they generate black list IP addresses and block these IP addresses at network switches or routers. The IP monitoring and blocking system enumerates IP addresses of top login successes and top login failures and updates them periodically. Managing the blacklist IP list requires high maintenance cost and applying Access Control Lists (ACLs) into network switches or routers is very difficult in the middle of system service. Moreover, when a hacker tries to connect to the game server by bypassing IP addresses using a virtual private network (VPN) or proxy IP, this method cannot prevent identity theft. Also, the user who uses similar IP addresses to blacklist IPs may get unfair damages.

To secure the system and network from the penetration of hackers, most online game companies operate intrusion detection systems (IDS), however, these detection systems are not specialized in detecting identity theft and in-game bugs. Also, IDS monitors network traffic, namely it adopts network-side detection methods such as network traffic monitoring or network protocol change, which can cause network overload and lags in game play.

Security solutions	Applicat-ion level	System failure	Prevent-ion	User Convenience	Vulner-ability
Firewall	Client	Low	Low	Convenient	High
Secure Keyboard	Client	High	Middle	Inconvenient	High
OTP /Security	Client	Middle	High	Very inconvenient	Low

card					
Intrusion detection system	Network	Middle	Middle	Low	High
IP monitoring and blocking	Server	Low	Low	Low	High
User notification system	Network	Low	Low	Middle	Middle

Table.2 Security solutions run by online game companies to detect identity theft

We summarized security solutions for identity theft detection proposed in previous works and adopted in the game industry in table.2. These approaches of the design with client-side solutions cause the user inconvenience and show low ability in detection and prevention. The network-side solutions such as suspicious logon IP monitoring and blocking can cause high maintenance costs, because the hackers usually change their IP address frequently. To overcome these drawbacks, a server-side detection method combined with domain knowledge and log data mining method is required.

3.2 Detection Model

To reduce the user inconvenience caused by client-side and network-side prevention methods, we propose a systematic and integrated model for server-side identity theft detection in online games. The proposed model integrates the domain knowledge about abnormal actions and data mining on game log data. From log data, we build up a well-balanced feature set that includes connection information, user behavior, and economy variables. Utilizing rich features along with appropriate problem-specific domain knowledge regarding the unique properties of identity theft will improve the detection accuracy.

Identity theft is not often detected until long after subsequent damage has occurred or users have noticed. To detect identity theft and prevent the damage that can be done to genuine users, it is important to recognize the pre-action of authentic stealing. In MMORPGs, a player controls several characters, which have their own assets. The character possesses some items and saves some items in inventory which exists in the game world. To check character wealth and set a target, hackers usually first explore the characters of a victim account. To view the assets of a character, hackers login to each character and check item lists, but they sometimes focus on checking, so they log out without stealing items. In online games, especially MMORPGs, since the character possesses items, monetization processes including taking off equipment, searching the inventory to find stored items, and selling items through various channels are required to monetize items. Finally, to achieve the main goal, hackers extort game money by buying a cheap item at an abnormally high price from another account, or selling an expensive item at a low price to another account. In the monetization process, the game money of a character decreases. These exploration and monetization processes can trigger an alarm informing the company that the user has been hacked.

In our model, the identity theft process is defined in detail and categorized into three steps of exploration, monetization, and theft from a close examination on real cases. There are five types of identity theft cases in MMOPRGs according to whether or not a hacker takes each step as shown in Fig.1. Some hackers explore victim characters and then leave without taking any items. In some cases, hackers explore and then monetize some items, but do not steal assets. These two cases happen mainly when characters don't possess expensive items, or the genuine user tries to log in. Aggressive hackers take all steps and spend considerable time in monetizing items. These types of hackers check all character assets, monetize items in many steps, and then steal the game money. Hackers who don't want to spend time in checking some character assets and then immediately take game money. Conservative hackers take the game money directly without exploration and monetization.

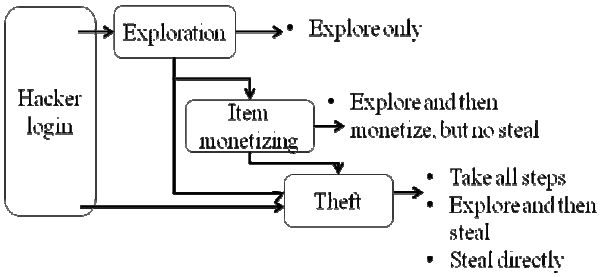

Fig.1 Process specification of identity theft

To process large-scale data and detect account hacking in real-time, we design an automatic identity theft detection model as shown Fig.2. First, we set up the feature set. We then perform the classification task using a decision tree to build up an efficient and understandable learning model. The performance of the learning model is evaluated in

terms of accuracy, precision, and recall. Since our proposed model can detect the pre-actions of exploration and monetization, the online game company can block the hacker login and warn the genuine user before items are stolen. In the worst case that authentic stealing happens directly, the company can report users quickly at least.

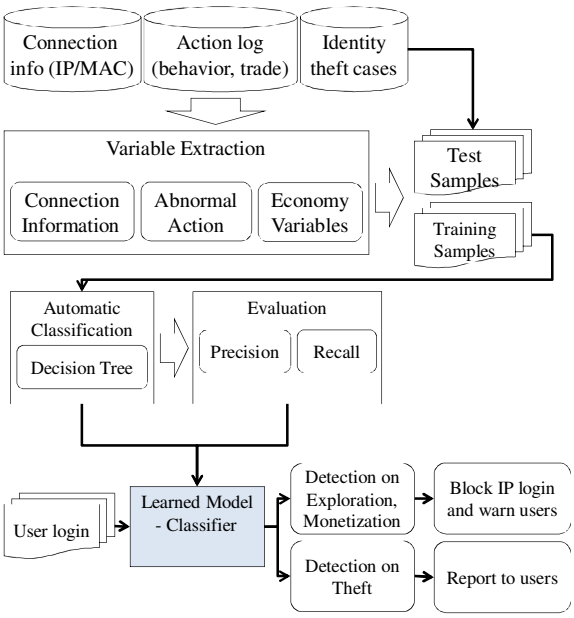

Fig.2 Automatic classification model for identity theft detection

3.3 Features for identity theft in MMORPGs

For identity theft detection, we adopt variables from connection information, user behaviors, and economy variables as shown in table.3.

Feature Type	Features	Characteristics
Connection information	IP & MAC entropy,	Generic
	IP distance	Generic
	VPN/PPTP	Generic
User Behavior	Recency, Frequency, Monetary (RFM) of abnormal action	Game-specific
	Logon time	Generic
	Trade with users who had been banned	Generic
Economy variables	Decreasing amount of money	Generic
	Increasing amount of experience points	Game-specific

Table.3 Features for identity theft detection in MMORPGs

We describe the variable definition in detail. When a user login, connection information such as IP and MAC address is retrieved and stored in an internal database in the company. As preliminary indicators that can recognize hacker logins, we adopt IP and MAC addresses being considered as personal identity in the computer network. Users who use dynamic IP addresses can have diverse IP addresses, but they have unique MAC addresses. In general, normal users do not have to change their MAC addresses using the same IP address. Even normal users who use dynamic IP addresses have similar IP addresses. Therefore, we develop metrics that measure the similarity of IP addresses and diversity of IP and MAC addresses.

When a user logs in with a new IP address, it is likely to be hacker login. An IP address consists of four classes separated by dot. Each IP class is named A, B, C, or D in sequential order. The distance between two IPs is calculated as follows. If all classes are fully equal then the distance is 0. If the C class is alike, 0.25. If the B class is alike, 0.5, and if the A class is alike 0.75. If everything is completely different, the score is 1. Some users who use dynamic IP addresses and log in at public places have diverse IP histories. However, IP addresses in the same place are usually same up to class C. Therefore, the IP distance is a good indicator of whether or not a new IP address is similar to a previous IP address.

To derive features from user connection information for identity theft, we adopt an information-theoretic measure, entropy [31]. It measures the uncertainty or impurity of data samples. It has been used in information science and started to be used in computer and network security contexts. Entropy-based measures have been proven to be good measures that numerate security vulnerabilities [4]. The users who log in with diverse IP addresses probably log in at diverse public places. The computers in public places are used by a large number of unspecified users and are disclosed to various hacking attacks. Therefore, the users with diverse IP and MAC addresses are more likely to be victims of identity theft than users with a limited number of IP and MAC addresses. As the preliminary indicators of identity theft, we measure the impurity of IP and MAC addresses using the entropy value. The entropy is larger when a user has diverse IP addresses in the connection history. The entropy reaches 0 when a user has limited IP addresses in history, i.e. when IP address history is pure. The entropy is expressed as the logarithm measures of the rates of IP occurrence from the connection history. Its value ranges between 0 and 1.

$$Entropy = \sum_{i=1}^{n} - p_i \log_2 p_i$$

$$P_i : \frac{\text{the number of connection with IP}_i}{\text{total connection s}}$$

Most Internet-related business companies have a set of rules to ban access from unauthorized IP addresses. Also, some online game companies allow access only from authorized IP addresses with an access control list of top level network backbone switches. These unauthorized IP addresses are updated periodically by security administrators, and they continuously update the IP addresses belonging to access-restricted countries. The company sets access-restricted countries for the following reason. Some countries try to leverage their economics by monetizing virtual assets of online games with low labor cost on a factory scale. Recent news media reports that China forces prisoners to play online games to obtain real currency [39]. To avoid being filtered, malicious users with restricted IP addresses try to log in by detouring. VPNs [40] can encrypt network traffic and hide IP addresses. Point-to-Point Tunneling Protocol (PPTP) is a method for implementing VPNs [38]. To detect the detoured access using VPN services, game servers have to generate logs including MAC addresses and 5 hops of traceroute information originating from each game client to the game server. Internal data-mining and manual inspections through monitoring personnel are used to detect detoured users using VPNs.

The main aim of hacking accounts is to steal game money and items and monetize them to real currency. Hackers usually target accounts that have expensive items and are high levels. Because they extract items or deprive money from victim accounts, their activities are limited to a few economic activities. Furthermore, to avoid being detected by genuine users, hackers speed up progress. In most cases of hacking involved in identity theft, automated programs break into a victim's account and takes game money and items for a short time. If users perform only economic activities just after they login, we speculate that they are probably hackers. We expect that the hacked account performs abnormal actions such as trading game money/items right after login. First, we define abnormal actions as economic activity such as trading and item monetization right after login. We define following actions as abnormal actions: scanning the characters' items, taking off equipment that characters are wearing, withdrawing items from inventory, trading with other users/sales agents/auction/NPCs (non-player character, characters controlled by the gamemaster), sending an email to other users, and receiving money from sales agents for the request of selling items. Second, we derive variables related to economic activities in recency, frequency, and monetary (RFM) terms [6]. RFM is a frequently-used set of metrics for analyzing customer buying behaviors in database marketing. R represents how recently the customer purchased, F how frequently the customer purchased, and M how much the customer spent through purchases. We adopt these metrics to describe hacker behaviors and to identify significant classifiers. In the context of identity theft detection, recency is the seconds that are taken until an abnormal action happens after login. Frequency is the interval between abnormal actions, and monetary is the incidence of an abnormal action. We calculate the recency, frequency, and monetary measures of pre-defined abnormal behaviors.

While RFM measures are derived from each abnormal action, we add two variables that are determined based on each character's login. We define the time difference between login and logout to reflect the speed of hacker actions. The other variable is set up to identify whether or not a user made a trade with an account who had been banned in this category. The stolen money will be transferred directly to attackers or passed on to attackers through other related users. Blacklist users, who had been accused of doing illegal activities such as using detoured VPN/PPTPs, game bots, or identity theft and banned for a while by the internal rules of the online game company, are probably involved in virtual crimes. We check to see whether or not users make trades with blacklists.

Regarding economic variables, we set up two features of the decreasing amount of game money and the increasing amount of experience points. The decreasing amount of game money will be a key classifier that determines whether or not a character login is hacked, since the main goal of hacking is to steal money. Players may lose money while they are playing a game normally when they lose in combat. In this case, the players still show a certain playtime and their experience points will also increase during that time. To differentiate between stealing game money and losing game money in gameplay, we add a game specific feature, the increasing amount of experience points. Since hackers don't play games while they are logged on, the increasing amount of experience points will be zero.

Most features adopted in our model for identity theft detection are generic. RFM values of abnormal actions become generic when the domain-specific abnormal actions are defined. The decreasing amount of experience points is definitely a game-specific feature. However, this feature that measures how user behavior fits the original purpose of the web site can be defined according to application domain. For example, in shopping sites, the number of viewing items can be employed instead of this feature. The model with generic features makes our model generic and applicable to other domains embedding a virtual economy.

3.4 Learning Model

For identity theft detection, we take a discriminative approach to learn the distinction between the normal and abnormal cases and to build up automatic classifiers. An automated system is necessary to process a large amount of log data. Simple, effective, and interpretable models are preferred in identity theft detection for practical use. In an online game company, using the detection method, a company blocks the account login when the account is recognized as compromised, while the company is contacting the genuine user. If the account is blocked wrongfully the conflict between users and the online game company can cause even legal problems. Therefore, the detection model should be conservative and can be interpreted in human words. To build the identity theft detection system based on efficient and understandable models, we adopt the decision-tree model. In the classification task, the neural network, support vector machine, and decision tree are widely adopted and are approved their good performance in previous works. The decision-tree model tolerates outliers and missing data and performs classification tasks in an efficient and quick manner. For processing multi-class categorical data, the neural network and SVM should create dummy variables for each level, and this adds to the computational burden while the decision tree does not [9]. The detection rules produced by neural network are hard to be interpreted and explained in human words. The SVM has a computation burden for the multi-class classification since it transforms the multi-class classification into multiple binary classifications. For the easy interpretation and lower computation burden, we employ the decision tree model.

The decision tree chooses one attribute of the data and splits its data into classes that generate the highest entropy reduction, or in other words, information gain [30].

$IG(S,A) = E(S) - \sum_i f(S_{ai}) E(S_{ai})$: information gain

$E(S) = -\sum_i f(s_i) \ln(s_i)$: entropy

$S = \{s \mid s_i \in S\}$: dataset

$A = \{a \mid a_i \in A\}$: attribute

$S_{a,i}$: dataset that belongs to the group seperated by attribute a_i

$f(s_i)$: the proportion of observations of s_i over total dataset

3.5 Evaluation

To evaluate the proposed model, we adopt two metrics that measure the classification performance. Recall is the probability that a positive case is correctly assigned; precision is the probability that an assigned positive case is correct. There is a natural trade-off between recall and precision. That is, if a model is tuned to increase recall, the precision usually decreases. Two metrics are defined as followings:

$$\text{Precision} = \frac{TP}{TP + FP}$$

: The probability that the predicted positive case is correct

$$\text{Recall} = \frac{TP}{TP + FN}$$

: Given a positive case,
the probability that it will receive the correct class

TP: true positive (correlty identified as identity theft)
TN: true negative (correlty identified as normal case)
FP: false positive (worngly identified as identity theft)
FN: false negative (wronly identified as normal case)

4 Experiments

We applied our detection model to a leading MMORPG company in Korea. This company maintains forty-three servers to host nearly 240,000 concurrent users at once. The research test-bed was set with log data from 01 Jun 2010 and 08 Jun 2010 recorded in a server. The company records around 70 million logs a day per server. During this period, 23 cases were reported as identity theft through the call center by users. Based on the results of the analysis on login IP and the investigation of damages, two cases were proven to be false reports. Some users file false reports after they lose expensive items. Also, some users give wrong time information about when identities are stolen.

As mentioned in Section 3, we divided the identity theft process into exploration, monetization, and theft. Based on the reported cases, we manually tagged character logins of victim accounts along

with three classes. Since an account has several characters, one account login includes several character logins. Reported cases are based on account login, but we performed the classification of character logins to specify the identity theft process. The classification results of total character logins including the 21 reported cases are shown in table.4. We performed the classification task on these four classes, where three classes were rare compared to the normal class.

Class	Character login frequency
Normal	378,041
Exploration	46
Monetization	29
Theft	32

Table.4 Class assignments of character logins

To perform the classification, we split the data set into training, validation, and test sets with a ratio of 0.5, 0.3 and 0.2 respectively. The classification rules are trained based on the training set and refined using the validation set. The test set is used to check whether or not output rules are over-fit to training data. The automatic classification using a decision-tree algorithm selected 11 variables from 29 variables as significant classifiers. The most important feature is the amount of money that decreases while a hacker is logged in to a victim's character. Then the connection information variables such as the IP/MAC entropy, distance, and VPN/PPTP are ranked high in terms of the importance value. The importance value of an attribute from a decision tree is relatively related to the reduction of the classification error by a branch of the attribute. The reduction of the classification error is the difference between the total classification error before an attribute splits the data set and the sum of the classification errors of each branch after the attribute splits the data set.

Variable description	Importance
Decreased amount of game money	1
IP entropy	0.9681
Mac entropy	0.7265
IP distance	0.7157
RFM – F of receiving game money for the request of selling items	0.5158
RFM – F of selling items	0.4241
Trade with accounts had been banned	0.3608
Difference between login and logout time	0.3410
RFM – R of game money decreased	0.2088
VPN/PPTP – detoured user	0.0990
RFM – R of buying items	0.0684

Table.5 Importance values of classifiers

The classification results are demonstrated in table.6. Since the normal cases are dominant in the current problem, the accuracy is more than 99%. We skipped the performance results for the dominant class for the same reason. The goal of the proposed model is to achieve high precision value and moderate recall value by increasing true positives and decreasing false positives at the same time. The online game company is very sensitive to false positives because it can cause disputes with users. Among three stages of identity theft, the classification for the monetization process outperforms with higher precision and recall values than the exploration and theft processes. We found that detection of theft showed the worst detection performance.

Performance measures		Value
Precision	Exploration	0.7222
	Monetization	0.8261
	Theft	0.4737
Recall	Exploration	0.2826
	Monetization	0.6552
	Theft	0.2813

Table.6 Classification performances

To justify the early detection ability of the proposed classification model based on process specification, we examined the identity theft cases according to the process specification. We classified the 21 users who filed identity theft as shown in Fig.3. Most hacking cases embedded the exploration and monetization processes. Only 3 hacking cases excluded two pre-processes before the authentic theft. In three cases, hackers did not explore the characters of a victim and did not repeat monetizing before taking game money. The result of the close examination of hacking cases implies that the detection of exploration and monetization activities will adequately secure the assets of victim accounts. Among 15 cases in which users suffered substantial damages from hackers, 11 cases exhibited the exploration process before theft, 9 cases exhibited the monetization process, and 8 cases exhibited both.

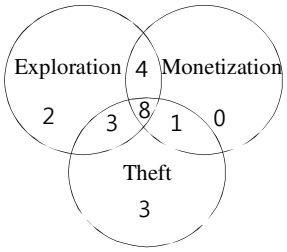

Fig.3 Classification of hacked users according to hacking process

The classification results give some implications about the security strategy in online game companies. To overcome the inconvenience of current prevention methods that require deploying security tools in the client side, it is necessary to employ server-side detection methods. To prevent user financial damage through identity theft, an online game company should deploy a detection system that detects abnormal exploration and monetization, blocks the malicious IP, and bans logins to the victim account before certifying genuine users. Connection-related features are identified as important classifiers, especially IP and MAC entropy, so that the strategy that filters abnormal user logins based on connection information should be established. Companies should monitor users with high IP and MAC entropy, check the IP distance when users log in with IPs totally different from user IP history, and apply the detection model to abnormal user logins.

5 Conclusions and Future research

We proposed a sever-side detection model for identity theft in online games. The proposed model classifies a hacker's login from a genuine user's login using well-balanced features from connection information, user behavior, and economic variables. The distance between IP, the entropy of IP and MAC address, the RFM measures of abnormal actions and economic variables are adopted in this model. We specified the identity theft process into exploration, monetization, and theft and posed identity theft detection as a multi-class classification task. Using a dataset extracted from a popular MMORPG of a major Korean game company, we performed the classification task using the decision tree model. We found that the detection on monetization has better performance than those on exploration and theft. Utilizing rich features, along with appropriate problem-specific domain knowledge regarding the unique properties of identity theft, contributes to good detection performance. The close cooperation with the industry, we could deliver the detection model and analysis results based on the real-world data to researchers. The server-side detection model will reduce the drawbacks such as system conflicts and user inconveniences of current prevention methods. It will also require fewer resources than the signature-based detection models that draw much attention from researchers. Regarding the practical contribution, the process specification and the automatic learning can provide the alarm about identity theft to the online game company and prevent substantial damage of the game user. In addition, the analysis on the importance of features enables the game company to build prevention strategy for the identity theft.

For future research, we will incorporate the network features in various possible networks in MMORPGs. The trade network, party-play network, and other social networks such as emailing and chatting will be considered. The consideration of network features will improve the detection accuracy on identity theft that is performed by acquaintances or friends. While most cases of identity theft occur through organized hackers who operate automated programs, some cases happen by acquaintances when users share personal information with others. Network features and node characteristics will be incorporated in the detection model of identity theft

Acknowledgements

This work was supported by the Ministry of Knowledge Economy, Korea, under the "ITRC" support program supervised by the National IT Industry Promotion Agency(NIPA-2011-C1090-1001-0004).

References

[1] S Abu-Nimeh and T Chen, Proliferation and detection of blog spam, *IEEE Security and Privacy*. 8(2010) 42.
[2] S Abu-Nimeh, D Nappa, X Wang, and S Nair, A Comparison of Machine Learning Techniques for Phishing Detection. In: Proceedings of eCrime '07 Proceedings of the Anti-Phishing Working Groups 2nd Annual Ecrime Researchers Summit. (2007) 60.
[3] MA Ahmad, B Keegan, J Srivastava, D Williams and N Contractor, Mining for gold farmers: Automatic detection of deviant players in MMOGs, CSE '09. International Conference on Computational Science and Engineering. 4(2009) 340.
[4] EM Airoldi, X Bai and BA Malin, An entropy approach to disclosure risk assessment: Lessons from real applications and simulated domains, Decision Support Systems. 51(2010) 10.
[5] J Bardzell, M Jakobsson, S Bardzell, T Pace, W Odom and A Houssian, Virtual worlds and fraud: Approaching cybersecurity in massively multiplayer online games, DiGRA. (2007) 451.
[6] RC Blattberg, Research opportunities in direct marketing, Journal of Direct Marketing. 1(1987) 7.
[7] S Bono, D Caselden, G Landau and C Miller, Reducing the attack surface in massively multiplayer online role-playing games, IEEE Security and Privacy. 7(2009) 13.
[8] KT Chen and LW Hong, User identification based on game-play activity patterns, NetGames'07 Proceedings of the 6th ACM SIGCOMM workshop on Network and system support for games (2007)
[9] KT Chen, JW Jiang, P Huang, HH Chu, CL Lei and WC Chen, Identifying mmorpg bots: A traffic analysis approach. (2006) 4.
[10] X Chen, I Bose, ACM Leung and C Guo, Assessing

the severity of phishing attacks: A hybrid data mining approach, Decision Support Systems. 50(2011) 662.
[11] YC Chen, PS Chen, J-J Hwang, L Korba, R Song and G Yee, An analysis of online gaming crime characteristics, Internet Research. 15(2005) 246.
[12] N Chou, R Ledesma, Y Teraguchi, D Boneh and JC Mitchell, Client-side defense against web-based identity theft, The 11th Annual Network and Distributed System Security Symposium (NDSS '04). (2004)
[13] OB Gaspareto, DAC Barone and AM Schneider, Neural networks applied to speed cheating detection in online computer games, ICNC '08. Fourth International Conference on Natural Computation. 4(2008) 526.
[14] S Gianvecchio, Z Wu, M Xie and H Wang, Battle of botcraft: Fighting bots in online games with human observational proofs, the 16th ACM conference on Computer and communications security. (2009) 256.
[15] J Hu, and F Zambetta, Security Issues in Massive Online Games. Security and Communication Networks. 1 (2008) 83.
[16] D Gunetti and C Picardi, Key stroke analysis of free text, ACM Transaction on Information System Security. 8(2005) 312.
[17] A Jain, A Ross and S Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology. 14(2004) 4.
[18] R Jamieson, and G Stephens. An Identity Fraud Model Categorizing Perpetrators, Channels, Methods of Attack, Victims and Organizational Impacts. In: Proceedings of Pacific Asia Conference on Information Systems (PACIS) (2007).
[19] MV Kesteren, J Langevoort and F Grootjen, A step in the right direction; bot detection in mmorpgs using movement analysis, The 21th Benelux Conference on Artificial Intelligence(BNAIC). (2009)
[20] J Ki, J Cheon and J Kang, Taxonomy of online game security, The Electronic Library. 22(2004) 65.
[21] HK Kim, S Hong and J Kim, Detection of auto programs for MMORPGs, AI 2005: Advances in Artificial Intelligence Lecture Notes in Computer Science. 3809(2005) 1281.
[22] HK Kim, Online game security, Codegate 2009 conference, http://www.hksecurity.net/home/pds/codegate2-1(huykang.kim).pdf,. (2009)
[23] S Li, C Chen and L Li, Using group interaction of players to prevent in-game cheat in network games, ISDPE '07 Proceedings of the The First International Symposium on Data, Privacy, and E-Commerce. (2007) 47.
[24] E Kirda, and C Kruegel, Protecting Users against Phishing Attacks. Computer Journal. 49(2005) 554.
[25] N Melnikov and J Schonwalder, Cybermetrics: User identification through network flow analysis, AIMS'10 Proceedings of the Mechanisms for autonomous management of networks and services, and 4th international conference on Autonomous infrastructure, management and security 6155/2010(2010) 167.
[26] S Mitterhofer, C Kruegel, E Kirda and C Platzer, Server-side bot detection in massively multiplayer online games, IEEE Security and Privacy. 7(2009) 29.
[27] HK Pao, HY Lin, KT Chen and J Fadlil, Trajectory based behavior analysis for user verification, Intelligent Data Engineering and Automated Learning-IDEAL 2010, LNCS. (2011) 316.
[28] A Peacock, X Ke and M Wilkerson, Typing patterns: A key to user identification, IEEE Security and Privacy. 2(2004) 40.
[29] K Prasetya and Z Wu, Artificial neural network for bot detection system in MMOGs, NetGames '10 Proceedings of the 9th Annual Workshop on Network and Systems Support for Games (2010) 16.
[30] JR Quinlan, C4. 5: Programs for Machine Learning. Morgan Kaufmann (1993).
[31] CE Shannon, and W Weaver, The Mathematical Theory of Communication. The Bell System Technical Journal. 27 (1948) 379.
[32] R Thawonmas, Y Kashifuji and KT Chen, Detection of MMORPG bots based on behavior analysis, The 2008 International Conference on Advances in Computer Entertainment Technology. (2008)
[33] J Vaidya and C Clifton, Privacy preserving association rule mining in vertically partitioned data, KDD '02 Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (2002) 639.
[34] WJ Wang, Y Yuan and N Archer, A contextual framework for combating identity theft, IEEE Security & Privacy. 4(2006) 30.
[35] RV Yampolskiy and V Govindaraju, Embedded noninteractive continuous bot detection, Computers in Entertainment (CIE). 5(2008) 1.
[36] J Yan and B Randell, An investigation of cheating in online games, IEEE Security & Privacy. 7(2009) 37.
[37] SF Yeung, JCS Lui, J Liu and J Yan, Detecting cheaters for multiplayer games: Theory, design and implementation, CCNC'06. 2(2006)
[38] http://www.faqs.org/rfcs/rfc2637.html.
[39] http://www.foxnews.com/scitech/2011/05/26/chinese-prisoners-forced-play-world-warcraft-detainee-says.
[40] http://www.vpnc.org/vpn--standards.html.

Jiyoung Woo received her Ph.D degree in Industrial Engineering from Korean Advanced Institute of Science and Technology in 2006. Currently she is a research professor in Graduate School of Information Security, Center for Information Security Technologies (CIST) in Korea University. Her research interests include Social Media Analytics and Online Game Security. Contact her at jywoo@korea.ac.kr.

Haw Jae Choi is taking Master degree course in Graduate School of Information Security, Center for Information Security Technologies (CIST) in Korea University. His research interests include Online Game Security and Intrusion Detection System. Contact him at chj870809@korea.ac.kr

Huy Kang Kim received his Ph.D degree in Industrial Engineering from Korean Advanced Institute of Science and Technology in 2009. Currently he is an assistant professor in Graduate School of Information Security, Center for Information Security Technologies (CIST) in Korea University. His research interests include Botnet Detection, Intrusion Detection System, Network Forensics and Online Game Security. Contact him at cenda@korea.ac.kr