User Identification based on Game-Play Activity Patterns*

Kuan-Ta Chen
Academia Sinica
ktchen@iis.sinica.edu.tw

Li-Wen Hong
Academia Sinica
ablazekandy@iis.sinica.edu.tw

ABSTRACT

Account hijacking is considered one of the most serious security problems in online games. A hijacker normally takes away valuable virtual items from the stolen accounts, and trades those items for real money. Even though account hijacking is not uncommon, *there is currently no general solutions to determine whether an account has been hijacked.* The game company is not aware of a hijack unless it is reported by the victim. However, it is usually too late—usually a hijacker already took away anything valuable when a user finds that his/her account has been stolen.

In this paper, we propose a new *biometric* for human identification based on users' game-play activities. Our main summary are two-fold: 1) we show that the idle time distribution is a representative feature of game players; 2) we propose the RET scheme, which is based on the Kullback-Leibler divergence between idle time distributions, for user identification. Our evaluations shows that the RET scheme achieves higher than 90% accuracy with a 20-minute detection time given a 200-minute history size.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User/Machine Systems—*Human factors*; K.8.0 [**Personal Computing**]: General—*Games*

Keywords

Account Hijacking, Biometrical Signatures, Kullback-Leibler Divergence, Online Games, User Behavior

1. INTRODUCTION

Security is considered one of the main problems in playing online games [17]. Among those security issues, *account hijacking* is considered critical and prevalent. Hijackers usually steal users' online game accounts by Internet phishing or Trojan horses [10]. Once a user's computer is infected by an "account collection" program, it resides in the system and monitors the user's input of accounts and passwords for logging into an online game. The intercepted accounts and passwords are transmitted to a server set up by a hijacker, who then enters the game with the stolen accounts, takes away valuable virtual items, and trades those items with other players for real currency. Even though account hijacking is not uncommon in a number of games, *there is currently no general solutions to determine whether an account has been hijacked.* The game company is not aware of a hijack event unless it is reported by the victim. However, it is usually too late—usually a hijacker already took away anything valuable when a user finds that his/her account has been stolen.

Moreover, an account may be *purposely* shared by a group of users for the sake of cost saving or information exchange, which increases the difficulty of demographical studies of games [4]. For instance, to further improve the design or pricing strategy of a game, game companies may analyze the effect of demographical factors on subscriber behavior, such as how players' age, gender, and occupations affect their payment behavior or the subscription period. Shared accounts affect the correctness of analysis results of such demographical studies. Likewise, account sharing also reduces game companies' ability of correctly providing personalized content for individual players [7].

The account hijacking and sharing problems are related to an more general issue of *Internet user identity management* [16]. Identifying who is the "true" human associated with an identify is one of the most difficult challenges in many Internet systems, especially those related to e-commerce. Until today, almost all Internet systems rely an account-password authentications to verify a user's identity. In case a user's account information leaks out to someone else, we have no ways to identify who is currently in charge of the leaked account, unless an effective and reliable biometrical signature is used [1, 5, 8].

In this paper, we propose a scheme to solve the identity theft and sharing problems by exploiting users' game-play activity patterns. The rationale behind our scheme is that, *the idle periods between successive moves of a player-controlled character can characterize a user's game-play characteristics.* For example, impatient and addicted players are likely to issue further movement commands before the previous one is finished, thus infrequent and short idle periods would intervene in successive movements. In contrast, leisure and casual players may involve in social interaction or out-of-game activities while the character is moving, thus

*This work was supported in part by Taiwan Information Security Center (TWISC), National Science Council under the grants NSC 95-2218-E-001-001, and NSC95-2218-E-011-015. It was also supported in part by National Digital Archives Program (NDAP), National Science Council under the grants NSC95-2422-H-001-024, and NSC 96-2422-H-001-001.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission from the authors.
NetGames'07, September 19-20, 2007, Melbourne, Australia.

the idle periods between successive movements tend to be long and occur frequently. Based on the activity logs of 287 players in a commercial game *Angel's Love*, we check the effectiveness of our proposed scheme. The RET scheme, which is based on the Kullback-Leibler divergence between idle time distributions, is shown to have reasonably good performance in user identification. Our evaluations shows that the RET scheme achieves higher than 90% accuracy with a 20-minute detection time given a 200-minute history size.

The remainder of this paper is organized as follows. Section 2 describes related works. We summarize our traces and analyze the general player activities in Section 3. In Section 4, we propose an identification scheme and demonstrate its ability in identity determination. In Section 5, we evaluate the performance of the proposed scheme with the consideration of the space and time requirement. Finally, Section 6 draws our conclusion.

2. RELATED WORK

To the best of our knowledge, this paper is the first to exploit users' game-play activities as a *biometric signature* for the account hijacking and sharing problems, thus there is no previous work on the same topic. The most related studies might be the two independent work by Yeung et al and Chen et al on game bot detection, which both are based on the discrimination between users' and game bots' behavior [3,18]. At the same time, a considerable number of works on biometric signatures and game player classifications are related to this study, which are summarized as follows.

Biometric signatures, which are traits related to a human as an identity, can be classified as *physiological* and *behavioral* signatures [1, 5, 8]. Physiological signatures are related to the characteristics of a human body, such as facial thermogram, hand vein, fingerprint gait, iris, and retina recognition. Behavioral signatures are related to the behavior of a person. The most commonly used behavioral signature is the handwritten signature. Other behavioral signatures include voice recognition, keystrokes, and mouse dynamics [6, 9, 13, 14].

The study of game player classifications is motivated by the need to provide personalized game content to individual players. That is, rather than enforcing all players undergo fixed narratives, the game can provide customized content for a player according to his/her own preference. Among the studies on player classifications, [7] discusses how to apply player classification to CRM (customer relationship management) and proposes memory-based reasoning to classify players as killers and non-killers. In [15], Thawonmas et al propose to cluster online gamers based on their movement trails using self-organizing map (SOM); their results show that the SOM can effectively cluster game players based on players' transition probabilities between landmarks.

3. PLAYER ACTIVITY ANALYSIS

In this section, we analyze the effectiveness of game players' activity patterns, i.e., the patterns a player-controlled character switches between *active* and *idle* states, in user identity determination. We start with a description of the player activity logs we collected. Next, we analyze the general player activity patterns in several aspects, including the active time and idle time distributions, and their representativeness of users' game-play characteristics. Finally, we close this section with a quick inspection whether the idle time distributions is an effective player signature for user identification.

Figure 1: A screen shot of the game *Angel's Love*

3.1 Data Description

We define *active period* and *idle period* as follows:

DEFINITION 3.1. *An* active period *of a game character is defined as a time interval* (t_1, t_2) *in which the character "continuously" moves, with a tolerance of discontinuity up to one second, i.e., the character does not stop over for any period longer than one second during* (t_1, t_2).

DEFINITION 3.2. *An* idle period *of a game character is defined as a time interval* (t_1, t_2) *in which the character has no movements, where* $t_2 - t_1 \geq 1$ *second.*

In this paper, we consider only the lengths of the active and idle periods, thus we shall use "active period" and "active time" interchangeably. The same rule applies to "idle period" and "idle time." In addition, for simplicity, we use the term "player" to refer to the virtual characters controlled by a human.

The player activity logs we use were recorded in a commercial MMORPG (Massively Multiplayer Online Role Playing Game), *Angel's Love* (see Fig. 1), developed by UserJoy Technology Co., Ltd.[1] The data collection was performed at one of the game servers by the game operational staff. During the trace period of 3 days, only a few randomly-chosen accounts were logged at a time to reduce the overhead of data logging. Player activity logs shorter than 200 minutes were removed to ensure high statistical significance. We summarize the collected player activity logs in Table 1, in which active/idle periods longer than 10 minutes are not counted, since we focus on players' short-term activity patterns.

3.2 General Player Activities

For a general idea of how active and idle periods distribute, we plot their density curves in Fig. 2. The graph shows that idle periods have a much wider distribution than active periods. It also reveals that the a significant proportion of active periods are shorter than 4 seconds, which indicates that players usually make short movements followed by a thinking time or non-movement activities.

[1]UserJoy Technology Co., Ltd., `http://www.uj.com.tw/`

Table 1: Summary of the player activity traces

Player #	Data Length	Activity Rate	Active Period	Idle Period
287	(7.0, 50.6, 67.1) hours	(0.35, 2.28, 5.12) cycle / min	(3, 6, 19) sec	(7, 18, 181) sec

† The (x, y, z) format denotes the (.05, .50, .95) quantiles of the respective metric.

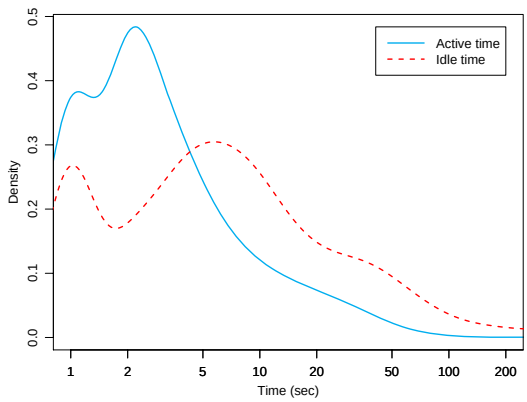

Figure 2: Distribution of active times and idle times of all players

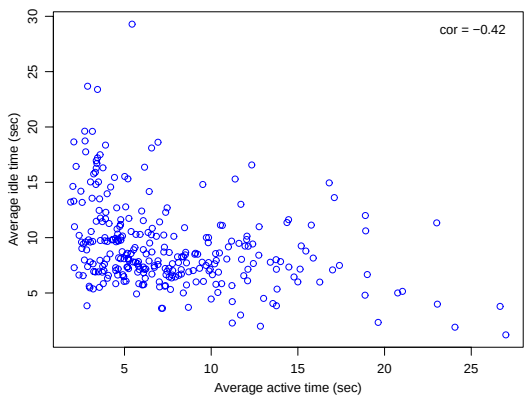

Figure 3: The average active time vs. average idle time of all players

We further examine the relationship between the average length of active periods and idle periods of each player. Because idle times can be extremely large (e.g., players may be away from their computers without quitting a game), we use a maximum active/idle time threshold to bound the magnitude of active and idle times. With the threshold set to 30 seconds, the active times and idle times have a strong *negative* correlation, as shown in Fig. 3. In other words, that if a player has a long average active time, then his/her average idle time tends to be short; so does the vise versa. This phenomenon indicates that *there is no typical length for both active and idle periods*, thus active players tend to have longer active periods and shorter idle periods than casual players do.

3.3 Comparison between Active and Idle Activities

We consider that the active time distribution and idle time

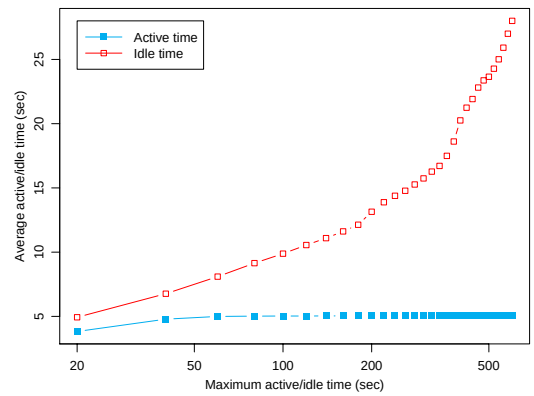

Figure 4: The average active time and idle time with varying maximum active/idle time thresholds

distribution should, to a certain degree, capture game-play characteristics of a user. Now that both distributions are highly correlated, it is likely that one of them is sufficient to reflect the highly variable player behavior. We argue that the idle time distribution is more representative of user game-play characteristics than the active time distribution with the following reasons:

1. *The idle time distribution captures more variability.* As depicted in Fig. 4, if we gradually relax the maximum active/idle time threshold, the average active time converges to around 5 seconds, while the average idle time keeps increasing unboundedly. This is reasonable because the length of active times is confined by the *game-play requirements*, e.g., players have to stop moving the characters in order to perform non-movement actions occasionally, and *human physical limits*, e.g., humans cannot perform continuous actions without any short break for a long time. In contrast, idle times can be extremely long by simply away from the computer without quitting a game. Thus, as idle times are not confined by the aforementioned restrictions those shared by all players, they would capture more *user-specific* game-play characteristics.

2. *Idle time process has smaller degree of auto-correlations.* We plot the lag-1 and lag-2 auto-correlation coefficients of the active time and idle time processes in Fig. 5. The results show that the active time processes for most players have moderate positive auto-correlations, which echoes the observation on temporal correlations of packet arrival processes in *ShenZhou Online* [2]. In contrast, the idle time processes for most players have very weak or no auto-correlations, which implies that the idle times are less dependent on the player's current status and tend to randomly distributed over time. Thus, the idle time distributions

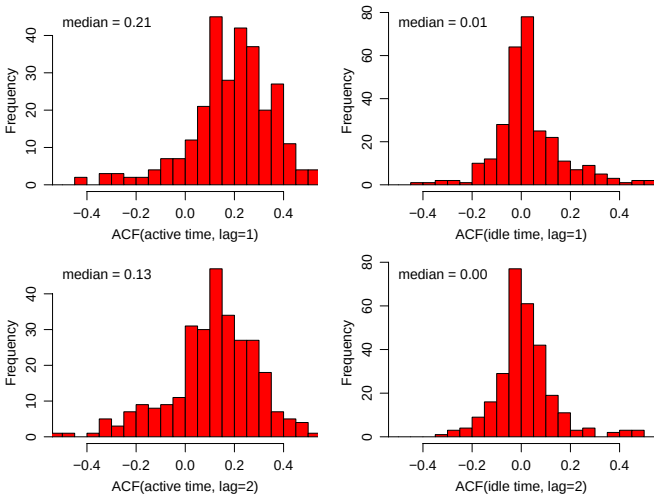

Figure 5: The autocorrelation coefficients of players' active time and idle time processes

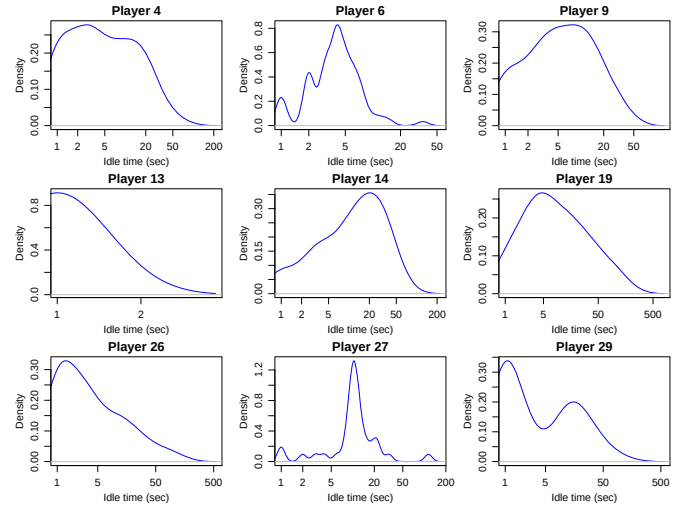

Figure 6: The idle time distributions of randomly selected players

would better capture a user's *time-independent* game-play characteristics than the active time distribution.

3.4 Idle Time Distribution as A Player Signature

We now to check whether the idle time distribution (ITD), which is one aspect of a user's activity patterns, can be used to distinguish different players. Fig. 6 shows the idle time distributions of 9 randomly chosen players. It can be seen that the ITD of each player shows a distinct pattern from the remaining players. The differences between those ITDs are not only in the central tendency, but also in the whole distribution (i.e., the shape). Specifically, some players (No. $4, 13, 19, 26, 29$) have left-skewed ITDs while others do not; some players (No. $6, 27$) have multiple modes while others have only one mode. No two players have equivalent idle time distributions from a strict view. This observation serves an initial evidence for our conjecture, that is, game-play activities can capture a player's personal traits, tendency, and characteristics, and therefore can be a biometrical signature for identity determination.

4. USER IDENTIFICATION SCHEMES

In this section, we aim to develop schemes for identifying users with their game-play activities. Based on the findings in Section 3.4, we propose the relative entropy test (RET) scheme, which is based on the relative entropies between two idle time distributions (ITDs). Via preliminary assessments, we show that the RET scheme is able to determine whether two segments of game-play activity records correspond to the same user with a reasonable accuracy.

The RET scheme is based on the Kullback-Leibler divergence [11] (KL divergence, or informally KL distance), also called information divergence or relative entropy, which measures the differences between two probability distributions. For probability distributions P and Q, the KL divergence of Q from P is defined to be

$$D_{\mathrm{KL}}(P\|Q) = \sum_i P(i) \log \frac{P(i)}{Q(i)}.$$

For a symmetric measure, i.e., the distance from P to Q is equivalent to the distance from Q to P, a symmetric version of the KL divergence is defined as

$$D_{\mathrm{SKL}}(P\|Q) = D_{\mathrm{SKL}}(Q\|P) = D_{\mathrm{KL}}(P\|Q) + D_{\mathrm{KL}}(Q\|P).$$

For simplicity, we shall use KL distance or KL divergence to denote their symmetric version.

We note that the magnitude of the KL distance cannot be interpreted except for the extreme case that $P = Q$, thus it cannot used to quantity "how close" two distributions are. However, we can determine the similarity between a set of distributions by indirect comparisons. For example, we can obtain that P and Q are more similar than Q and R if $D_{SKL}(P, Q) < D_{SKL}(Q, R)$.

In the RET scheme, we use the KL distances between idle time distributions to determine the identity of a user. We conjecture that though the ITDs of a user over time may be slightly different, but their differences *converge to a user-specific value*, which quantifies the "variability" of the user game-play behavior across time periods. In other words, the RET scheme will determine two sets of ITDs are from two users if their KL distances cannot converge to the same median. In the following, we discuss the algorithms and the effectiveness of the RET scheme in the aspects of consistency and discriminability respectively.

4.1 Consistency

The RET scheme operates on a set of ITDs, rather than on a single ITD. Assuming a player has n idle time subsequences of length t seconds, which correspond to n ITDs. We randomly choose k out of n ITDs, and compute $C(k, 2)$ KL distances between each pair of the k ITDs, so a distribution of KL distances is obtained. (For simplicity, we shall use KLD to denote the distribution of KL distances between ITDs.) This procedure is run for $m = \lceil n/k \rceil$ times and thus m KLDs are obtained. As a demonstration, we plot the KLDs from four players in Fig. 7. As can be seen, the KLDs of a user have similar shapes and concentrate to the same median. On the other hand, the general shapes of KLDs of different players are dissimilar, which initially supports our

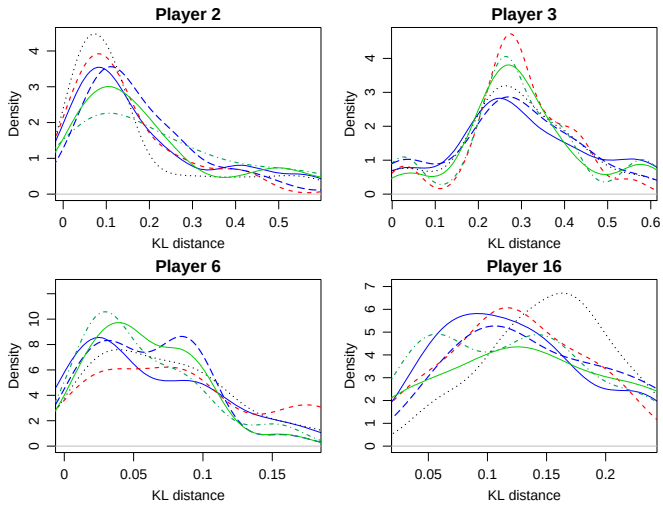

Figure 7: Selected players' KL distances of their idle time distributions in different time periods

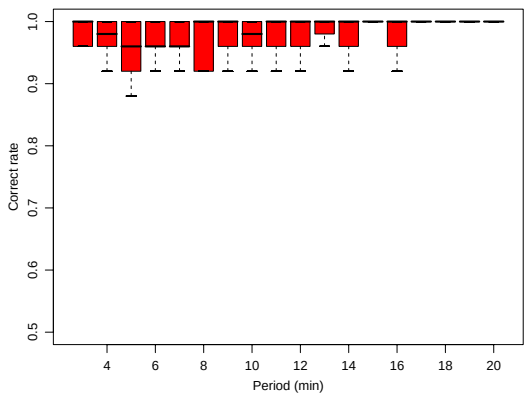

Figure 8: The correct rates of the consistency test for the RET scheme

conjecture that the convergence of KLDs can be a signature for user identification.

To perform a consistency check, we set $k = \lfloor n/2 \rfloor$ so that $m = 2$ KLDs are obtained for each player. Next, we determine whether the two KLDs from a player have the same median by the Mann-Whitney U test (also called the Wilcoxon rank-sum test or Wilcoxon-Mann-Whitney test) [12], which is a non-parametric test for assessing whether two distributions have statistically equivalent medians. This test is chosen because the median is a much more robust estimator of the central tendency of a sample. We use a two-sided Wilcoxon test with a significance value of 0.05, and the correct rate is computed as the ratio that the two KLDs of a user pass the test (i.e., the two KLDs have statistically equivalent medians).

Fig. 8 plots the correct rate versus the time period t. This graph reveals that the correct rate is generally higher than 0.95 no matter how long the time period is and evidences the good consistency property of the RET scheme.

4.2 Discriminability

We now turn to checking the discriminability property of

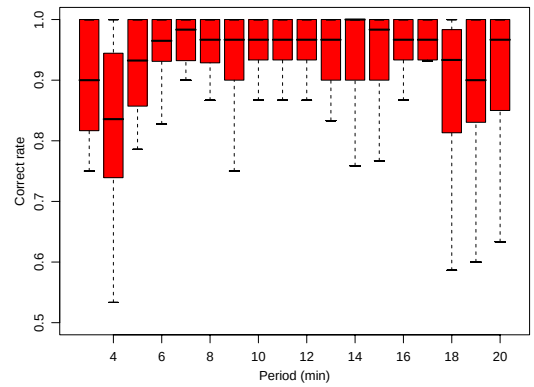

Figure 9: The correct rates of the discriminability test for the RET scheme

the RET scheme. Assuming we have N players, each of which has n_i ITDs. We compute $\text{KLD}_{i,j}$ as the distribution of the $n_i n_j$ KL distances between the n_i ITDs of player i and the n_j ITDs of player j. The discriminability test between two players i and j is done by applying a one-sided Wilcoxon test on $\text{KLD}_{i,i}$ and $\text{KLD}_{i,j}$ with a null-hypothesis that the latter is significantly larger than the former. The correct rate is so defined as the proportion of tests passed among the $C(N, 2)$ Wilcoxon tests.

We find that the correct rate of the discriminability test is generally good (higher than 0.9) regardless of the length of the time period, as shown in Fig. 9. Combining with the results in Fig. 8, both consistency and discriminability tests manifest the efficiency of the RET scheme in correctly identifying users based on their idle time distributions in a game.

5. PERFORMANCE EVALUATION

So far we have shown that the RET scheme performs reasonably well in both consistency and discriminability checks in Section 4. Here we conduct a more detailed evaluation of the performance of the RET scheme with the considerations of the effect of *the detection time* and *the history size*.

We assume a practical scenario that our schemes would take place: The user identification system records the idle times of each player in a database with a maximum recording time of T_{rec} minutes. Whenever a player joins a game with a valid account, the system records all the idles times the player makes, and performs the identification procedure after s/he joining the game for T_{obs} minutes. The importance of the two factors T_{rec} and T_{obs} in the identification system is as follows:

- T_{rec} decides how long the player activity history should be kept in the system database. According to our traces, each activity cycle (an active period followed by an idle period) takes about one minute on average, such that a maximum history size of T_{rec} minutes correspond to T_{rec} idle times. Assuming we have one million user accounts, $T_{rec} = 200$ minutes, and each idle time uses 4 bytes, then totally 800 MB of storage space is required.

- T_{obs} decides how quickly a newly joined player can be re-authenticated with the game-play activities. Longer

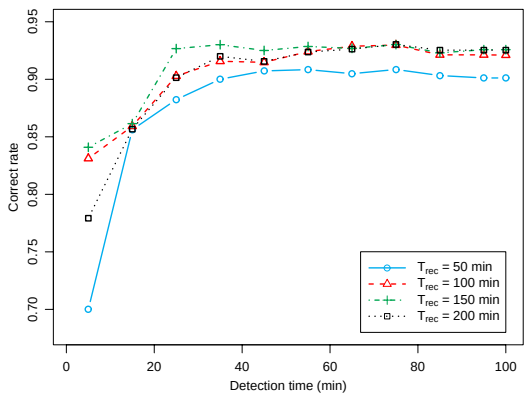

Figure 10: The evaluation results of the RET scheme with considering the history size and detection time

> T_{obs} brings two disadvantages: 1) if the current session is used by an account hijacker, then the system cannot detect the account theft except the session is longer than T_{obs} minutes; 2) the idle times of active sessions must be stored in the main memory, that brings some memory overhead to the system. Assuming $10,000$ players are online, and $T_{obs} = 30$ minutes, then approximately 1.2 MB of main memory is needed for storing the idle times of those to-be-identified players.

We evaluate the identification accuracy of the RET scheme with different combinations of detection time and history size. As shown in Fig. 10, larger history size and longer detection time both increases the detection correct rate. We consider that generally a small T_{obs} is more preferred than a small T_{his}, as long detection time reduces the chance for identifying the players associated with short game sessions. Consequently, if we fix the history size to 200 minutes, the detection accuracy is higher than 0.9 for a detection time of 20 minutes.

6. CONCLUSION AND FUTURE WORK

In this paper, we aim to solve to account hijacking and share problems in online gaming. Our contributions are three-fold: 1) we propose the idea of user identity determination based on game-play activities; 2) we show that the idle time distribution is a representative feature of game players; 3) we propose the RET scheme, which is based on the Kullback-Leibler divergence between idle time distributions, for user identification. Our evaluations shows that the RET scheme achieves higher than 90% accuracy with a 20-minute detection time given a 200-minute history size.

Even though our results show that the idle-time-based scheme performs reasonably well if we can observe a player for 20 minutes, hijackers may not stay online for such a long time. In practice, they may need a few minutes to take away virtual items valuable from the stolen account. We believe that by utilizing more aspects of game-play activities, such as movement patterns, and the way users control the character to do a specific action (via mouse or keyboard), the game-play-activity-based schemes can be further extended for a more efficient and reliable biometrical signature for human identification.

Acknowledgments

This work would not have been possible without the extensive trace of *Angel's Love*. The authors are much indebted to Tsing-San Cheng, who helped us gather the trace. The authors also acknowledge anonymous referees for their constructive criticisms.

7. REFERENCES

[1] A. Broemme. A classification of biometric signatures. In *IEEE International Conference on Multimedia & Expo*, 2003.

[2] K.-T. Chen, P. Huang, and C.-L. Lei. Game traffic analysis: An MMORPG perspective. *Computer Networks*, 50(16):3002–3023, 2006.

[3] K.-T. Chen, J.-W. Jiang, P. Huang, H.-H. Chu, C.-L. Lei, and W.-C. Chen. Identifying MMORPG bots: A traffic analysis approach. In *Proceedings of ACM SIGCHI ACE'06*, Los Angeles, USA, Jun 2006.

[4] M. D. Griffiths, M. N. Davies, and D. Chappell. Demographic factors and playing variables in online computer gaming. *CyberPsychology & Behavior*, 7(4):479–487, Aug. 2004.

[5] D. Guinier. Identification by biometrics. *SIGSAC Rev.*, 8(2):1–11, 1990.

[6] D. Gunetti and C. Picardi. Keystroke analysis of free text. *ACM Trans. Inf. Syst. Secur.*, 8(3):312–347, 2005.

[7] J.-Y. Ho, Y. Matsumoto, and R. Thawonmas. MMOG player identification: A step toward CRM of MMOGs. In *Proc. of the Sixth Pacific Rim International Workshop on Multi-Agents*, pages 81–92, Nov 2003.

[8] A. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):4–20, Jan 2004.

[9] R. Joyce and G. Gupta. Identity authentication based on keystroke latencies. *Commun. ACM*, 33(2):168–176, 1990.

[10] D. M. Kienzle and M. C. Elder. Recent worms: a survey and trends. In *WORM '03: Proceedings of the 2003 ACM workshop on Rapid malcode*, pages 1–10. ACM Press, 2003.

[11] S. Kullback and R. A. Leibler. On information and sufficiency. In *Annals of Mathematical Statistics*, volume 55, pages 79–86, 1951.

[12] H. B. Mann and D. R. Whitney. On a test of whether one of two random variables is stochastically larger than the other. *Annals of Mathematical Statistics*, 18:50–60, 1947.

[13] A. Peacock, X. Ke, and M. Wilkerson. Typing patterns: A key to user identification. *IEEE Security and Privacy*, 2(5):40–47, 2004.

[14] M. Pusara and C. E. Brodley. User re-authentication via mouse movements. In *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 1–8. ACM Press, 2004.

[15] R. Thawonmas, M. Kurashige, K. Iizuka, and M. Kantardzic. Clustering online game users based on their trails using self-organizing map. In *Proceedings of ICEC 2006*, pages 366–369, Sep 2006.

[16] J. R. Vacca. *Identity Theft*. Prentice Hall PTR, 1 edition, Sep. 2002.

[17] J. Yan and B. Randell. A systematic classification of cheating in online games. In *Proceedings of ACM SIGCOMM 2005 workshops on NetGames '05*. ACM Press, 2005.

[18] S. Yeung, J. C. Lui, J. Liu, and J. Yan. Detecting cheaters for multiplayer games: Theory, design and implementation. In *Proceedings of IEEE International Workshop on Networking Issues in Multimedia Entertainment (NIME'06)*, Las Vegas, USA, Jan 2006.