Vol. 49 No. 1 IPSJ Journal Jan. 2008

Regular Paper

Anomaly Detection on Mobile Phone Based Operational Behavior

Takamasa Isohara,[†1] Keisuke Takemori[†2] and Iwao Sasase[†1]

Information protection schemes on mobile phones become important challenges because mobile phones have many types of private information. In general, user authentication and anomaly detection are effective to prevent attacks by illegal users. However, the user authentication can be applied only at the beginning of use and the conventional anomaly detection is not suited for mobile phones, only but computer systems. In this paper, we propose a simple and easy-to-use anomaly detection scheme on mobile phones. The scheme records the keystrokes as the mobile phone is operated, and an anomaly detection algorithm calculates a score of similarity, to detect illegal users. We implemented a prototype system on the BREW (Binary Run-time Environment for Wireless) emulator and evaluated error rates by using results from 15 testers. From experiments results, we show the proposed scheme is able to apply the anomaly detection by checking the similarity score several times.

1. Introduction

Recently, mobile phones have many convenient functions such as e-mail, address lists, electronic money transfers, online banking services, and electronic tickets. Because several kinds of personal information are managed on a mobile phone, it is important to protect personal information from illegal users who are not the owner of a mobile phone. In general, two approaches are implemented on a computer system to protect the data against intruders; authentication and anomaly detection.

Authentication can effectively reduce attacks by keeping illegal users from entering the system. Two types of authentication are applied for the mobile phone platform, namely password authentication and biometrics. The password authentication has a low cost and is easy to use. This scheme checks the user's knowledge of the confidential information. A user only needs to memorize a short password and can be authenticated anywhere, anytime, regardless of the types of access devices he/she employs [1]. The biometrics checks for automatic recognition of people based on their distinctive physiological characteristics such as face and fingerprint [2)–5)]. This scheme could form a component of an effective user authentication, because the physiological characteristics intrinsically and reliably represent the individual's bodily identity. Biometric characteristics cannot be lost or forgotten; they are quite difficult to copy, share, and distribute; and they require the person being authenticated to be physically present at the time and point of authentication. However, this authentication acts at initial device operation. If the authentication procedure is passed, the device is freely operated by not only the legal user but also illegal users, thus all private information in the device becomes open to attackers [6].

To deal with this type of security concerns, anomaly detection, which acts as the second protection system, could effectively help detection of illegal users. The anomaly detection systems have been applied in various areas to monitor anomaly incidents as network packets, system calls and user behaviors [7]. Especially, anomaly detection techniques are actively researched for the computer system because unknown usage can be detected by using normal behavior-based profiles. By this technique, normal profiles of user behavior are created and compared with the current user activities. If a significant deviation is observed, the system raises an alarm. The conventional technique of behavior-based anomaly detection focuses on the rhythm of keystroke patterns or transition probability of commands that are used to operate the computer system. Anomaly detection algorithms takes a statistical approach that requires complex calculations.

However, the conventional user behavior-based anomaly detection is not applied to mobile phones because mobile phones use different types of interfaces from the QWERTY-array keyboard, and has a limitation of calculation

†1 Department of Information and Computer Science, Keio University
†2 KDDI R&D Laboratories

resources. In fact, the following are observed on a mobile phone operation environment: the number of keys on the mobile phone are limited, and the conventional anomaly detection algorithm needs robust calculation resources, such as CPU power and memory usage.

In this paper, we propose an anomaly detection scheme to detect illegal user operation, which focuses on the frequency of keystroke records. The scheme records the keystroke in the background process. The keystroke records are divided into a long-term profile and a short-term profile. The anomaly detection algorithm calculates the frequency of keystrokes from the long-term profile to make a legitimate user profile. We compare the long-term profile with the short-term profile to detect illegal user operation. We implemented a prototype system on the BREW emulator, and then, evaluated the False Acceptance Rate (FAR) and False Reject Rate (FRR) of our scheme. The results show that our proposed scheme can detect the illegal users and prevent personal information leakage.

The paper is organized in six sections. Section 2 describes related works and considers requirements for anomaly detection on mobile phones. Section 3 proposes the anomaly detection algorithm. Section 4 explains the implementation techniques for the BREW platform. Section 5 shows evaluation results of the proposed scheme and discusses the advantage of our system. Lastly, we conclude in Section 6.

2. Related Work and Problems in Applying Them to the Mobile Phone

In this section, we explain related works about the behavior based anomaly detection techniques for the computer system and point out the problems in applying them to mobile phones.

2.1 Anomaly Detection Overview

The basic assumption of an anomaly detection system is that the illegal user's actions differ from the behavior of a legitimate user. In the first stage, a profile of normal activity is built. The second stage is an analysis between normal activities and the current user's activity. If abnormal activity is detected, the system takes multi-modal security measures such as generating an alert or locking the device by authentication schemes.

In anomaly detection, two types of mistakes are possible; normal behavior is incorrectly assessed as illegal (false positive), or an illegal penetration attempt into a system is taken as normal activity (false negative).

Anomaly detection has been applied at various levels such as network packets, system calls and user commands. In this paper, we discuss user behavior-based anomaly detection because our goal is protecting the information on mobile phones.

2.2 User Behavior Based Anomaly Detection

Some researchers have been published in the anomaly detection via user behavior.

References 8) and 9) propose keystroke-based anomaly detection. This method is used in the personal computer environment. It has compatibility with mobile phones because the method does not interrupt device operation. It collects the operation history which is called the "keystroke record" of the device at the time of user operation, and the anomaly detection algorithm analyzes the rhythm of keystroke patterns. For example, the latency between pressing and releasing a key is analyzed.

Reference 9) uses keystroke patterns to train a neural network approach. Reference 10) focuses on the operational habits of a mouse device and the anomaly detection system uses a Bayes-network approach to make a legitimate user profile. On the neural network and the Bayes-network approaches, the relationship between a legtimate user profile, and the authentication results, must be trained.

On the other hand, Ref. 11) uses a finite automata approach that is calculated by a state transition model. The processing load of the state transition model is too heavy for mobile phone.

In Ref. 12), the anomaly detection system uses a frequency-based learning that analyzes a series of user commands for the personal computer, and constructs user profiles that include a cycle of command repetition. Because the conventional frequency-based approach must analyze many commands to authenticate a legitimate user, it has not been applied to mobile phones.

These methods have the following advantages; first, the device operation is not interrupted by the authentication procedure because the user only has to use the device as per usual. Second, the method is easy to implement on the device because the method requires only a keyboard.

2.3 Problems for Applying Anomaly Detection to Mobile Phones

Conventional user behavior-based anomaly detection is designed for computer systems. There are two principal differences between computer systems and mobile phones. First, the format of the keyboard which is used to input the user command to the system is different. The computer system uses a full-size keyboard which is called the "QWERTY-array" keyboard. QWERTY-array keyboards have about 100 keys. On the other hand, the number of keys on a mobile phone's keyboard is limited. In general, a mobile phone's keyboard consists of the numeric pad and cursor keys and there are about 25 keys. Second, the computer system is operated by command sequence. Command sequence consists of alphabetical letters. Examples of commands in a UNIX system include "ls", "pwd" and "vi filename.txt". Therefore, many commands are used in computer systems. In contrast, the number of commands on a mobile phone is very limited. A mobile phone and its applications are driven by receiving the key code that corresponds with the key on the mobile phone. Therefore, the number of commands in mobile phone corresponds one-to-one with the number of keys on the mobile phone.

Also, anomaly detection algorithms that are used on the conventional scheme need robust calculation resources such as CPU power and high memory requirement because the design of the algorithms are based on the computer system. On the other hand, a mobile phone has limitations to calculation resources.

The requirements for a user behavior-based anomaly detection scheme on a mobile phone are as follows:

(1) Analysis of the operation tendencies in mobile phones.
(2) An anomaly detection algorithm which is suitable for the mobile phone's calculation resources.

3. Proposed Anomaly Detection Scheme

In this section, we propose an operation behavior based anomaly detection scheme, which does not require excessive processing resources on the mobile phone. We describe the system model and explain the mechanisms of anomaly detection on a mobile phone.

3.1 System Model

Figure 1 shows a system model of an anomaly detection scheme. The proposed scheme consists of 4 modules, namely 1) the keystroke record module, 2) the data preprocessing module, 3) the anomaly detection module and 4) the response module.

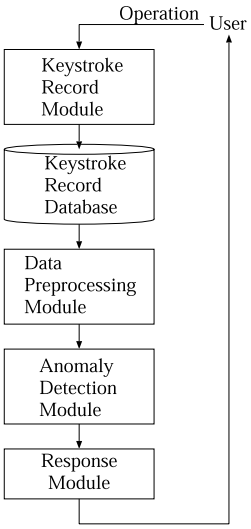


Fig. 1 System model of anomaly detection scheme.

- Keystroke record module: Keystrokes recorded on a mobile phone are captured by this module and stored in the keystroke record database. The keystroke is recorded at the time the mobile phone is operated. By using this approach, the record is obtained without interrupting the device operation, and hence, the mobile phone user only has to operate the mobile phone as per usual. Details of this module are described in Section 3.2.
- Data preprocessing module: Before the anomaly detection processing, the keystroke record that is stored in the keystroke record database is divided into two categories; the short-term profile and the long-term profile. Details of this module are described in Section 3.3.
- Anomaly detection module: The anomaly detection algorithm is contained in this module. We propose a frequency-based anomaly detection algorithm. Details of this module are described in Section 3.4.
- Response Module: When abnormal activity is detected on the anomaly detection module, the response module suspends the system and requires authentication from the user.

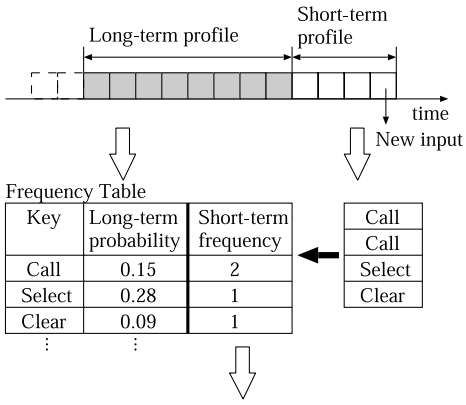


Fig. 2 An definition of profiles.

3.2 Keystroke Record Module and Data Structure

The first step of anomaly detection scheme is collecting the data that are used for anomaly detection. In order to take out the complexity and hesitation for usage of this scheme, we select the data that we are able to collect at the same time as the mobile phone is being operated. The Keystroke record module collects the sequence of the key codes. The Key code is the unique value that corresponds one-to-one with the physical button on the mobile phone. The collected key codes are stored in the keystroke record database and are processed by the data preprocessing module and the anomaly detection module.

3.3 Data Preprocessing Module

The second step of the anomaly detection scheme is data preprocessing. Before the anomaly detection, several data preprocessing are necessary.

The keystroke record is divided into two parts, one is a short-term profile and the other is a long-term profile.

Figure 2 shows the short-term and the long-term profiles. The short-term profile is a data set that is used to authenticate a legitimate user, and it consists of a certain number of keystroke records from the latest operation of the mobile phone. The long-term profile is used to evaluate the short-term profile, and it does not include the short-term profile.

Also, the long-term profile is larger than the short-term profile, and it contains operational trends of the legitimate user.

Fig. 3 An example of key groups.

3.4 Anomaly Detection Module

The anomaly detection algorithm is implemented from this module. To detect an abnormal activity, we introduce a similarity score that determine if there is abnormal activity. This score is calculated using the following two steps.

First, we make a frequency table for each key by using the long-term profile. We propose the following two approaches to calculate the frequency table.

Key Group Based Approach In this approach, keys on the mobile phone are divided into groups to reduce the memory usage needed to manage the frequency tables of the keystroke records. The number of groups is defined by the semantics of applications on the mobile phone. **Figure 3** shows an example of key group definitions. In this example, keys on the mobile phone are divided into two groups; a cursor key group and a numerical key group. Because there are two types of applications on the mobile phone, one is operated by the whole keys, and the other is operated by only cursor keys.

Individual Key Based Approach To achieve higher accuracy for anomaly detection than the key group based approach, the frequency of individual key presses is calculated. By using this technique, we can estimate more fine-grained probability than with the key group based algorithm.

Based on these approaches, the frequency table for keys or key groups is as follows;

$$P_k = F_k / L_{long-term\_profile}, \quad (1)$$

where F_k is the number of records in the long-term profile for key group k, and $L_{long-term\_profile}$ is the length of the long-term profile.

Second, we estimate a similarity score by

comparing the frequency table of keys or key groups with the short-term profile. The score of similarity is calculated as follows;

$$S = \sum_{k=1}^{m} (P_k \cdot N_k) / L_{short-term\_profile}, \quad (2)$$

where m is the number of groups or all keys implemented on the mobile phone, P_k is the frequency that key k is pressed, N_k is the number of appearances of key k in the short-term profile, and $L_{short-term\_profile}$ is the length of the short-term profile.

Here, we compare the amount of memory usage to create the frequency table in each Approach. The data format of the frequency table is shown in Fig. 2. In the case of the Key Group Based Approach, the frequency table has the same number of entries as the number of key groups. In the case of the Individual Key Based Approach, the frequency table has the same number of entries as the number of keys on the mobile phone. In the case of Fig. 3, the mobile phone has 2 groups and 21 keys. Based on these assumptions, the Key Group Based Approach reduces the memory usage by 1/10 that of the Individual Key Based Approach.

This approach is based on following two assumptions; 1) the operational behavior is different between a legal user and an illegal user, 2) if the same user creates a short-term profile and a long-term profile, the trends are the same in both profiles. Therefore, when both profiles are created by the same user, the similarity score is high. **Figure 4** shows a distribution of similarity scores. In addition, the similarity score is automatically maintained to adequate value, because the scope of long-term profile is defined to have some certain records from short-term profile and the record in long-term profile slides one by one by user's command input.

To detect an abnormal activity, the system continuously checks the similarity score. The system calculates the similarity score several times, and for checks abnormal activity. If abnormal activity is detected, based on the similarity score being higher than a predetermined number, the system responds by forcing a password authentication by the user.

4. Implementation

4.1 Implementation Platform

We developed a prototype system on BREW emulator [13]. BREW is one of the standard application platforms on a mobile phone. **Figure 5** shows the architecture of the BREW platform. The developer can create a BREW applet on the BREW platform.

The BREW platform is in a single task environment that is able to execute only one applet and has an implementation scheme called "Extension". Extension is in the set of common program libraries such as DLL in the Microsoft's Windows environment or dynamic shared object in the PC-UNIX environment.

In the current BREW environment, the accuracy of the timer is low. Thus, anomaly detection based on intervals of time cannot be used. When the implementation environment is arranged, we can examine this kind of method in the future.

4.2 Module Placement

We implemented a prototype system by using the extension technique. The Extension module includes the keystroke record module, the data preprocessing module and the anomaly detection module. **Figure 6** shows the structure of the prototype system.

4.3 Implementation on Emulator

We used the BREW emulator to implement the prototype system. The emulator runs on the Windows platform and emulates the BREW application platform. Developers can run BREW applets and extensions. **Figure 7** shows a screen shot of the BREW emulator. **Table 1** shows the size of the modules.

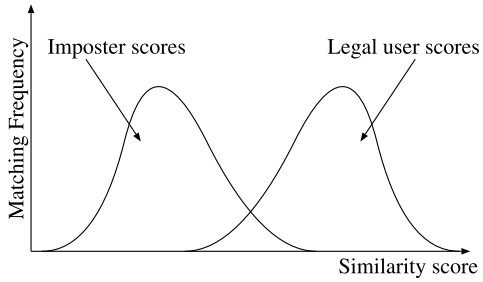


Fig. 4 The distribution of similarity scores.

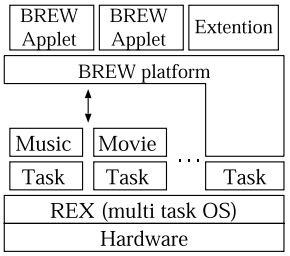


Fig. 5 Structure of BREW platform.

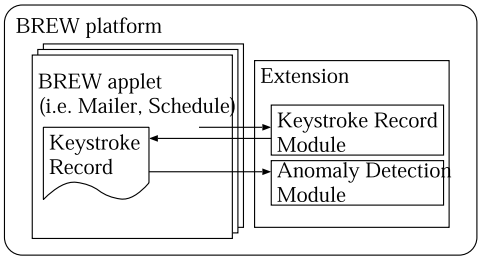


Fig. 6 Structure of prototype system.

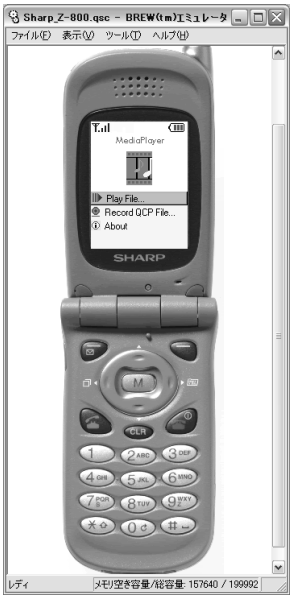


Fig. 7 Screen shot of the BREW emulator.

Table 1 Size of modules.

Module	Size
Extension module	204 Kbyte
Database (500 records)	5.26 Kbyte

5. Experimental Results

We carried out experiments to check error rates of the proposed scheme. This section describes the experimental conditions, the experimental results and the discussion.

5.1 Experimental Condition

This experiment was done by using the BREW emulator. There is an operational difference between an emulator and a real machine. However, our proposed scheme focuses on the historical characteristics of the keystroke record, and our proposed scheme does not focus on the timing of the keystroke record, such as latency, and therefore, there is no necessity to consider the differences in the operation.

Based on the operation method, we classify mobile phone applications into two types. Type 1 refers to applications which are operated by specific keys. This type of application is able to be operated by only selecting items. Type 2 refers to applications which are operated by all the keys on the mobile phone. This type of applications requires input using text or numeric keys. To compare these application's operational behavior, we used the media player and cashbook in our experiments. Media player plays music and is an example of type 1. Cashbook handles mobile phone owner's household account, and is an example of type 2.

15 testers participated in this experiment. First, the testers practiced the operation of the emulator and the test bed application. Second, the testers made long-term profiles for themselves. These profiles were used as each user's operational characteristics. Third, they were free to operate applications, thus to calculate the similarity score. They implemented these tasks ten times.

Table 2 The number of calculations.

Algorithm	Phase 1	Phase 2
Key group-based	604	4644
Individual key based	65	605

5.2 Number of calculations of the Anomaly Detection Algorithm

We propose two approaches in the anomaly detection algorithm, a key group-based approach and an individual key based approach. The number of calculations is different in these approaches because the number of data sets to anomaly detection is different in them. Here, we compare the number of calculations.

The anomaly detection procedure is divided into two phases, in phase 1, a table is made from the long-term profile, and in phase 2, the long-term profile is compared with the short-term profile. In our scheme, the number of groups is 2 as shown in Fig. 3 and the number of keys that are implemented on the mobile phone is 22. The length of the long-term profile and the length of the short-term profile are assumed to be 100 and 10, respectively. **Table 2** shows the number of calculations in each approach. From Table 2, we can show that the computational complexity of the Key group based algorithm is higher than the computational complexity of the Individual key based algorithm.

5.3 Error Analysis of The Proposed Scheme

Using the keystroke record collected from the

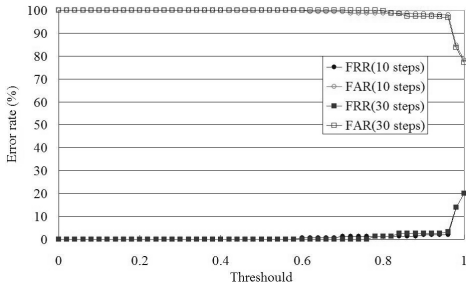


Fig. 8 Error rate of proposed scheme on media player in the case of key group approach.

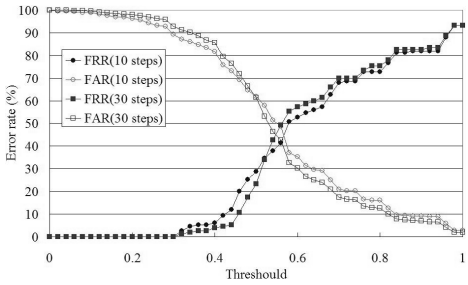


Fig. 9 Error rate of proposed scheme on cashbook in the case of key group approach.

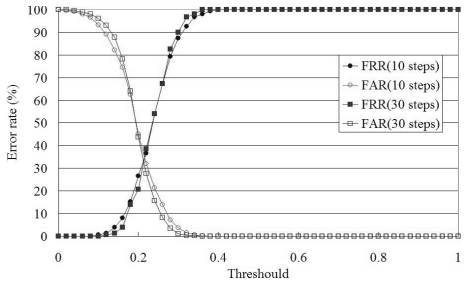


Fig. 10 Error rate of proposed scheme on media player in the case of individual key approach.

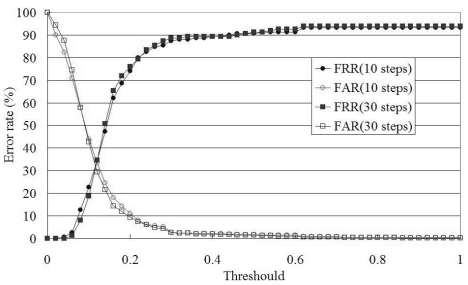


Fig. 11 Error rate of proposed scheme on cashbook in the case of individual key approach.

experiments, we estimated a detection rate of abnormal activity. Here, we introduce three indicators that are used for the abnormal activity detection.

- False Reject Rate (FRR): the percentage of incorrectly rejected legal users.
- False Acceptance Rate (FAR): the percentage of illegal users incorrectly matched as a legal user.
- Equal Error Rate (EER): determined by finding the point where FRR intersects FAR.

In the experiments, the length of the long-term profile is set to 100 records. The FRR and the FAR when the length of the short-term profile is 10 records and 30 records are estimated.

Figures 8 and **9** show the FRR and FAR in the case of the key group-based approach for media player and cashbook, respectively. And, **Figs. 10** and **11** show the FRR and FAR in the case of the individual key based approach for media player and cashbook, respectively. The X axis shows the decision threshold and the Y axis shows the error rate. The decision threshold is equal to the similarity score which is shown in Fig. 4.

These error rates are estimated by the 15 testers experiments. To evaluate the error rate of the anomaly detection system, more testers are required. Thus, these results contain a sampling error. In Fig. 8, the EER is not shown because the utilized buttons in media player are concentrated into one group. In Fig. 9, EER is 45%. On the other hand, in Figs. 10 and 11, EER is shown as 35%. The error rate of our scheme depends on the uniqueness of the long-term profile. Thus, the anomaly detection rate is improved by putting the characteristic operations into the long-term profile.

In our scheme, anomaly activity is detected by checking the similarity score several times. Here, the number of checks for the similarity score is set to 5, and the abnormal detection threshold is set to 3. In fact, if abnormal activity is detected by the anomaly detection algorithm, 3 times, the user is locked out. In Figs. 10 and 11, the EER is shown to be 35%. Thus, an illegal user is detected 65%. Based on this assumption, the anomaly detection rate is the sum of the probability that the abnormal activity will be detected five times, four times and three times. And, it is calculated as follows,

$$\begin{aligned} & P(anomalydetection) \\ &= {}_5C_5 \cdot 0.65^5 \cdot 0.35^0 \\ &\quad + {}_5C_4 \cdot 0.65^4 \cdot 0.35 \\ &\quad + {}_5C_3 \cdot 0.65^3 \cdot 0.35^2 \\ &= 0.76 \end{aligned} \tag{3}$$

From the results, the rate of anomaly detection is expected to be 76% by checking the similar-

Table 3 authentication latency

	Key Group Based	Individual Key Based
1	18 msec	16 msec
2	19 msec	15 msec
3	20 msec	16 msec
4	17 msec	14 msec
5	18 msec	15 msec
avg.	18.4 msec	15.2 msec

Table 4 Million Instructions Per Second

CPU	MIPS
BREW (ARM9 processor)	220
Pentium4 2.4 GHz	4423

ity score several times. This rate is insufficient to authenticate the user by only this scheme. Thus, it is necessary to combine this with another authentication method for more reliable information protection.

Even when the user passes the password attestation, information is protected by combining the authentication method and proposed scheme. And, if the attack to biometrics [14] is done, the proposed scheme acts as second protection system on the mobile phone.

5.4 Analysis of Overhead Costs

In this section, we estimate the authentication latency on the BREW mobile phone by using experimental results on the BREW emulator. Most functions between the BREW emulator on the personal computer and the BREW mobile phone are similar except processing speed. Therefore, we can estimate the authentication latency on the mobile phone by evaluating the authentication latency of the BREW emulator on the personal computer and by comparing the processing speed between the personal computer and the mobile phone.

Table 3 shows the results of authentication latency on the BREW emulator. In these results, the length of the long-term and short-term profiles are 100 and 30, respectively. And, **Table 4** shows the Million Instructions Per Second (MIPS) of the BREW mobile phone and the personal computer that is used to run the BREW emulator [15),16)].

From Table 4, the MIPS of the BREW mobile phone is about 1/20 times faster than that of the personal computer. In the case of the BREW mobile phone, the authentication latencies of the Key Group and the Individual Key Based Approaches are estimated as 380 msec and 300 msec, respectively. In addition, the 380 msec and 300 msec are worst case because we do not consider the overhead of the BREW emulator on the personal computer. Therefore, our proposed approaches can be applied to the BREW mobile phone.

6. Conclusion

We have proposed the operational behavior-based anomaly detection for mobile phones. The proposed scheme collects keystroke records and calculates the similarity between the short-term profile and the long-term profile in order to detect illegal users. Also, we consider both the key group approach and the individual key approach, because CPU and memory resources are limited on the mobile phone.

We evaluated our proposed scheme on the BREW emulator. In this evaluation, media player and cashbook are implemented as test bed applications. 15 testers created their long-term profile, and the error rates were estimated by doing the comparison between 15 short-term profiles and 15 long-term profiles, ten times. We evaluated the FAR and FRR, and show the error trade off of the proposed scheme. By using the individual key approach, the EER in both applications is 35%, and we show that the proposed scheme can be used to trigger executing the password authentication on the mobile phone. Because the scheme does not have to interrupt the operation of mobile phone, it is expected that it can be easily applied to mobile phones.

Acknowledgments This work was supported by the Global COE Program "High-Level Global Cooperation for Leading-Edge Platform on Access Spaces (C12)".

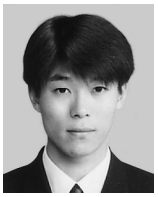
References

1) Korff, Y., Hope, P. and Potter, B.: *Mastering FreeBSD and OpenBSD Security*, Oreilly & Associates Inc. (2005).
2) Jain, A., Bolle, R. and Panakanti, S.: *Biometrics: Personal Identification in Network Society*, Kluwer Academic Publishers (1999).
3) Tian, Y.-L., Kanade, T. and Cohn, J.F.: Recognizing Action Units for Facial Expression Analysis, *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.23, No.2, pp.97–115 (2001).
4) FOMA F901iS: http://www.nttdocomo.co.jp/product/foma/901i/f901is/topics_01.html (2006).
5) FOMA P901iS: http://www.nttdocomo.co.jp/product/foma/901i/p901is/topics_03.html (2006).
6) Sun, B., Yu, F., Wu, K., Xiao, Y. and Leung,

V.C.M.: Enhancing Security using Mobility-Based Anomaly Detection in Cellular Mobile Networks, *IEEE Trans. Vehicular Technology*, Vol.55, No.4, pp.1385–1396 (2006).
7) Chinchani, R., Muthukrishnan, A., Chandrasekaran, M. and Upadhyaya, S.: RACOON: Rapidly Generating User Command Data For Anomaly Detection From Customizable Templates, *Proc. 20th Annual Computer Security Applications Conference* (2004).
8) Joyce, R. and Gupta, G.: Identity Authentication Based on Keystroke Latencies, *Comm. ACM*, Vol.33, No.2, pp.168–176 (1990).
9) Cho, S., Han, C., Han, D.H. and Kim, H.-I.: Web-Based Keystroke Dynamics Identity Verification Using Neural Network, *Journal of Organizational Computing and Electronic Commerce*, Vol.10, No.4, pp.295–307 (2000).
10) Izumi, M., Nagao, W., Miyamoto, T. and Fukunaga, K.: User Identification System Using Feature of Mouse Operation, *IEICE Trans. Comm.*, Vol.J87-B, No.2, pp.305–308 (2004).
11) Shirai, H., Nishino, J., Odaka, T. and Ogura, H.: An Intrusion Detection Technique Using Characteristics of Command Chains in an Interactive Computer Environment, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, Vol.J82-A, No.10, pp.1602–1611 (1999).
12) Odaka, T., Shirai, H., Nishino, J. and Ogura, H.: An Authentication Method Based on the Cycle of the Command Repetition, *IPSJ Journal*, Vol.42, No.10, pp.2533–2536 (2001).
13) Qualcomm BREW Home: http://brew.qualcomm.com/brew/en/ (2006).
14) Matsumoto, T., Matsumoto, H., Yamada, K. and Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems, *Proceedings of the Conference Optical Security and Counterfeit Deterrence Techniques IV, Part of IS&T/SPIE's Electronic Imaging 2002*, Vol.4677, pp.275–289 (2002).
15) ARM: http://www.arm.com/ (2007).
16) SiSoftware Zone: http://www.sisoftware.co.uk/ (2007).

(Received May 30, 2007)
(Accepted October 2, 2007)
(Online version of this article can be found in the IPSJ Digital Courier, Vol.4, pp.9–17.)

Takamasa Isohara received B.E. and M.E. degrees in the Department of Information and Computer Science from Keio University, Yokohama, Japan in 2005, 2007, respectively. He joined KDDI R&D Laboratories in 2007. His current research interests include network security.



Keisuke Takemori received B.E. and M.E. degrees in Electrical Engineering, and Ph.D. degree in Information and Computer Science, all from Keio University, Yokohama, Japan in 1994, 1996, and 2004, respectively. He joined KDDI R&D Laboratories in 1996. His current research interests include communication network and internet security. He is a member of IEEE and IEICE.

Iwao Sasase received B.E., M.E., and Ph.D. degrees in Electrical Engineering from Keio University, Yokohama, Japan in 1979, 1981, and 1984, respectively. From 1984 to 1986, he was a Postdoctoral Fellow and Lecturer of Electrical Engineering, the University at Ottawa, Canada. He is now a Professor of Information and Computer Science at Keio University, Japan. His research interests include modulation and coding, mobile communications, satellite communications, optical communications, communication networks, and information theory. He has published more than 220 journal papers and 314 international conference papers. He received the 1984 IEEE Communication Society Student Paper Award (Region 10), 1986 Inoue Research Award, 1988 Hirosho Ando Memorial Young Engineer Award, and 1996 IEICE Switching System Technical Group Best Paper Award. He is a senior member of IEEE, the Information Processing Society of Japan, and the Society of Information Theory and Its Applications (SITA), Japan.