Towards Implicit Enhancement of Security and User Authentication in Mobile Devices Based on Movement and Audio Analysis

Hamed Ketabdar, Mehran Roshandel, Daria Skripko
Deutsche Telekom Laboratories, TU Berlin
Ernst-Reuter-Platz 7, 10587, Berlin, Germany
{hamed.ketabdar, mehran.roshandel, daria.skripko}@telekom.de

***Abstract*—In this work, we present initial investigations towards analysing movements of a mobile device as well as ambient audio captured by the mobile device for enhancing security functionalities in the device. We present a few scenarios which can lead to security threats related to data or services on a mobile device (e.g., a phone being lost or stolen). We show how unexpected movements or ambient audio captured by the device can deliver information which can be important considering security issues, and reveal those scenarios. In addition, we present how the identity of a user can be verified (or identified) by his mobile device based on pattern of his regular physical activities such as walking. This allows for implicit and continuous re-identification of the user. The implicit process does not require active participation of user, and allows for authentication during regular daily activities. The proposed method can also be used to complement regular authentication techniques to protect for example an open account on a mobile phone. It can also help to reduce number of re-authentications by verifying that the mobile device is continuously operated by the same user since the last regular authentication. Our final goal is to come up with a correlation model describing the relationship between movements of a mobile device as well as ambient audio, and security related issues.**

Keywords-Security; Mobile Devices; Motion and Audio Analysis; Embedded Sensors; Unexpected Events; Implicit Authentication

I. INTRODUCTION

Mobile devices are one of the essentials in our daily life used for communication, storage and service access. As mobile devices technology develops, they are used more and more for storing different data, text, audio, photos, etc. Obviously, some of this data can have private or confidential content. In addition, mobile devices are also becoming a gateway to connect with many different services such as Email, E-banking, etc. Most of these services can also be related to business, confidential or private aspects of user's life. Unfortunately, there is always a risk that these confidential data or services are exposed to unauthorised people, for instance when a mobile phone is lost or stolen.

If a person left his Personal Digital Assistant (PDA) or smartphone in a cab, a power-on password would prevent anyone who found it from casually browsing content, racking up calls, and using his email account. However passwords can be shared, guessed, or stolen. Enforcing minimum password length and complexity rules can make password authentication more effective, but they do not improve usability. Compared to laptops, PDAs and smart phones are used far more frequently, for much shorter tasks, demanding near-instantaneous availability. Authentication methods that get in the way of using these frequently used shorter tasks are disabled. This is the main reason why Personal Identification Number (PIN) is unused on mobile devices. Convenience often trumps security, especially if nothing enforces policy [1]. The same argument can also be applied to other means of authentication such as finger print [2], face profile [3], voice based verification [4], etc. All these approaches are intermittent and therefore susceptible to attack, e.g., an unauthorized user can access a portable computer either by stealing a password or exploiting an open account of a user [5].

In this work, we propose a new paradigm for increasing security of data and service access on mobile devices, based on analysis of movement and audio data captured by the device. The new paradigm allows for online, implicit and continuous protection of data without the burden of involving the active attention of the user. We show that analysis of audio and physical movement data captured by a mobile phone can indicate unexpected events which can lead to having the phone being lost or stolen. In addition, we show that analysis of audio and physical movement data during regular physical activities (e.g., walking) by the user can allow for authenticating/identifying the user. The proposed method is an implicit authentication technique, i.e., it does not involve active attention of the user, and it is performed continuously as user is regularly using or carrying the device. Physical movement data can be captured by accelerometer sensors embedded in modern mobile devices. Audio data is captured by embedded microphone.

Such a paradigm can be used to increase security of data and service access on mobile devices as a stand-alone technique, or as complementary to regular authentication techniques. It can for instance protect an open account from an unauthorised user. In addition, as complement of regular authentication techniques (e.g., PIN, signature, finger print), the number of regular re-authentications can be reduced if our method detects that the same user has been continuously using the device. Moreover, the implicit security protection process can be used to implement a "Graded Security" scheme for data and service access. In this scheme, a security level score is calculated based on the outcome of audio and movement analysis. According to the calculated security level, different access policies can be established. This scheme allows protecting data and services according to their importance and security threat level of mobile device.

 ISBN: 978-1-61208-117-5

The paper mainly studies two cases related to audio and movement analysis for enhancing security functionalities in mobile devices. The first case is detecting unexpected events which can lead to having the mobile device being lost or stolen. This is for instance the situation that a phone falls accidentally out of the user's pocket/bag and is left unattended. The second case is using audio and movement analysis for user identification/authentication. In this case, movement and audio data captured during physical activities of the user is used as a basis for his identification. We talk about the first case in Section 3, and the second case in Section 4.

II. ANALYSIS OF MOVEMENT AND AUDIO DATA

Information about movement of the mobile device is obtained by analysis of data provided by integrated acceleration sensors. These sensors are originally used for automatic screen rotation and navigation [6, 7, 8]. Acceleration sensors integrated in a mobile device provide linear acceleration information along the x, y and z directions. The acceleration sensed by the mobile device can be due to different sources. In this work, we are mainly interested in components of acceleration caused by physical activities of user, or unexpected events such as free falls, impacts, etc. According to our experiments, these components usually appear in high frequency content of acceleration signals. Lower frequency components can be mainly due to gravity force, as well as movements of the user in a vehicle. In most of the cases, we pre-process the acceleration signals with a time derivative operation which effectively acts as a high pass filter.

Audio data is also captured using the microphone embedded in the mobile device.

In order to analyse data captured by the accelerometer or microphone, we usually extract some features from the data in certain time intervals (windows). These features are mainly based on average, variance, and rate of change of recorded signals in the interval. For instance, the average of norm of acceleration signals (along x, y and z directions) in a time interval can indicate the level of physical movement of the device in the interval.

III. UNEXPECTED EVENT DETECTION

Unexpected events experienced by a mobile device can be a sign of security threats. In this section, we review a few unexpected scenarios which can lead to security threats related to mobile devices. We further discuss how these situations can be detected based on analysis of captured motion and audio information using sensors and microphone embedded in a mobile phone.

We start with a simple but practical case. If a mobile phone accelerometer has not detected motion for a relatively long period of time, it may indicate that the phone is lost or forgotten somewhere. This may result in a security risk for data or services accessed by the phone. This situation can be easily identified by analyzing motion data obtained from the embedded acceleration sensors. In this case, the rate of change of acceleration data can be quite low over a long period of time. Upon detection of such a situation, the device

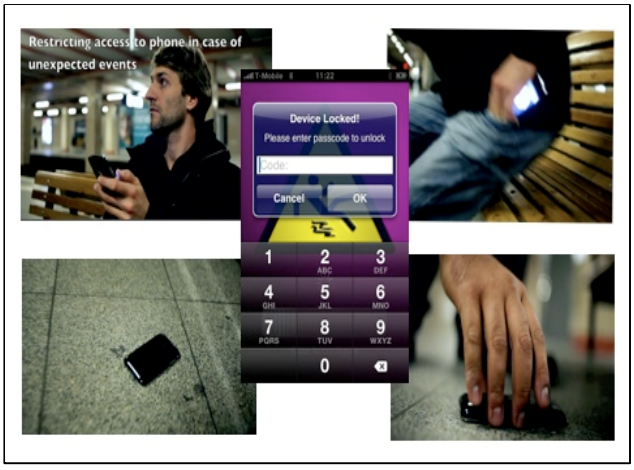

Figure 1. A mobile phone under risk of being lost or stolen.

can be locked requesting user re-authentication.

Another risky situation can be when the user is engaged in high level of physical activity (e.g., running or sports). In such a situation, attention of user to his mobile phone may be reduced, resulting in a relatively higher risk of losing the device. Detecting such a situation based on embedded accelerometer sensors allows setting security options on the mobile device to a higher level. According to our experiments (assuming that the mobile device is carried somewhere on the user body), the average and variance of acceleration show significantly high values in these cases, as compared to regular situations.

A common risky situation which can lead to having the device lost or stolen is when the mobile device falls out of user's pocket or bag, and is left unattended for a while (Fig.1). The user may not notice what has happened to the device due to distractions with other activities. We have studied detecting such a scenario based on analysing audio and acceleration information. We model this unexpected event based on three sub-events: free-fall, shock (impact with floor), and no activity (movement) after the shock. When the phone falls, it initially experiences a free fall situation. Upon hitting the floor, it experiences a shock. However, this is not enough for identifying the situation as "risky", because the user may immediately pick up the phone. Therefore, it is also necessary to check for a period of "no activity" after the shock.

We have setup user studies to evaluate our algorithm for detecting the last mentioned scenario. The experimental setup is similar to [9]. We have used iPhone 3G for the experiments. Acceleration and audio data is recorded using embedded microphone and sensors through a data collection application developed for iPhone. For the experiments, we have recorded a database of normal and risky (as defined) situations. In this database, there are 98 samples of normal situations, and 36 samples of physical shocks. In order to obtain physical shock, we let the iPhone to fall on a carpet or wooden floor form a distance of approximately 75 cm. In order to obtain normal condition samples, we let 5 users to carry the iPhone normally in their pocket, hand or bag for a

 ISBN: 978-1-61208-117-5

TABLE I. RESULTS FOR DETECTION OF A RISKY SITUATION WHICH CAN LEAD TO HAVING A MOBILE DEVICE BEING LOST OR STOLEN.

Algorithm	Accuracy	True Alarm	False Alarm
3 step definition	**94.4**	34	4
Only impact	86.1	31	9

period of 10 seconds. These users indulge in different day-to-day activities such as walking, jogging, taking lift and walking on stairs. We tried to have different variety of scenarios, especially those which can have similarity to a shock (due to high physical activity) such as walking on stairs and taking lift. In this way, we can make sure that our algorithm is able to distinguish between such cases and a real risky shock [9].

As mentioned earlier, the risky situation is defined as a sequence of free fall, impact (shock), and no activity period. The free fall is detected when the norm of acceleration signals (along x, y, and z directions) falls below a predefined threshold. The no-activity period is identified when the average of norm of acceleration signals in an interval after the impact (8 seconds in our case) falls below a threshold. The impact (shock) situation is detected by comparing features extracted from acceleration and audio data against a statistical model created for impact (shock). The model which is used for this work is a Multi-Layer Perceptron (MLP) trained using samples of shock (impact) and regular situation collected as previously mentioned. The features used in this study are mainly based on average and variance of acceleration components (as well as their norm), and audio signal. The MLP is then able to classify new samples of features as shock or normal (regular) situation. The "risky situation" is detected upon detection of free fall, shock, and period of no-activity in correct order. Table 1 summarizes initial results. Our studies show that defining the three steps for risky events detection can significantly reduce number of false alarms (Table 1). The first row in the table shows the results when the three step definition is used, and the second row shows results when only impact is considered as risky event.

IV. IMPLICIT IDENTITY VERIFICTION/IDENTIFICTION BASED ON AUDIO AND MOVEMENT ANALYSIS

Another possibility for using audio and movement analysis in enhancing security functionalities in mobile devices is for user authentication/identification based on regular user's physical activities such as walking. When the mobile device is carried by the user (e.g., in his pant pocket), it can capture samples of audio and motion information, and check for a biometric patterns in them. In this way, the identity of the user can be verified in a continuous and implicit manner. The authentication is implicit, so the user does not need to actively participate in authentication process. The user only performs his regular activities and the authentication method looks for a biometric sign in his pattern of physical activities. As discussed before, this implicit authentication method can be used alone or as complementary to regular authentication methods. The device can automatically detect that it is not being carried or operated by the same user anymore, therefore switch to a higher level of required authentication. As a side advantage, this technique can reduce required number of normal authentications. If the device implicitly detects that it has been continuously used by the same person since the last authentication, it may not ask for a new authentication process for the same service. This reduces the number of repetitive re-authentication. In addition, an implicit authentication score estimated based on audio and movement analysis can be used to set up different security threat levels for the mobile device, allowing implementation of a graded security scheme.

In the following, we present our initial experiments for user identification/authentication based on data captured by a mobile device (audio and motion) during regular physical activities. We show that users can be classified with high accuracy based on captured information using a mobile phone in their pant pocket.

V. EXPERIMENTS AND RESULTS

We set initial experiments to investigate possibility of implicit user authentication/identification based on regular physical activities of user (walking in our case).

For experiments, we recorded device motion information (using embedded acceleration sensors) as well as ambient audio (using embedded microphone). The recoding is done during regular physical activities which are walking in this case. The device is carried in user's pant pocket. We have used iPhone as mobile device and we recorded the signals using a data collection application we developed for iPhone.

We have invited 9 participants for the experiments. We captured audio at 8 KHz and acceleration at 50 Hz using embedded sensors in the iPhone. We let the iPhone to be placed regularly in the pocket, without fixing its position or orientation. The test users are asked to walk for about 2 minutes in indoor and outdoor environments. The recording for each user is repeated over 3 different days. Users were asked to come for the experiments with different sets of shoes and pants in different days, in order to take into account the effect of variability in clothing in the identification process.

Feature extraction is the first processing step. We extract two sets of features, one from acceleration signals and one from audio signal. Features are extracted over a window of 2 seconds of acceleration and audio signals. For acceleration signals, the extracted features are mainly based on average, variance and magnitude of acceleration components. Here is a list of features:

- Average field strength along x, y, and z directions.
- Variance field strength along x, y, and z directions.
- Average of Euclidian norm of filed strength along x, y, z.
- Variance of Euclidian norm of field strength along x, y, and z.
- Piecewise correlation between field strength along x and y, x and z, and y and z.

 ISBN: 978-1-61208-117-5

For audio signal, extracted features are mainly based on average, variance, and energy of the audio signal in each window. Variance of Fourier transform of audio signal is also used as a feature.

Extracted features are feed as input to MLP for user classification/identification. Table 2 shows classification results for different feature sets. We report results for using movement (acceleration) based features, audio based features, and a combination of movement and audio based features. As can be seen from the table, the combination of audio and movement based features provide the best user identification results (90.1%). Table 2 shows identity verification (authentication) measures for some of the users. The Receiver Operating Characteristic (ROC) measurements show a good tradeoff between true and false alarms indicating significant user authentication results.

In this experiment, we have presented initial results for user identification/authentication over a window period of 2 seconds. This means that every 2 seconds, we are able to re-authenticate the user. However, such a short interval continuous re-authentication may not be necessary in practical applications. It may be enough to have an authentication measure for instance, every minute. In such a case, short interval (2 seconds window) based authentication results can be used in a voting scheme. The identified user over a minute is the user having highest vote (recognition) in 2 second based windows. Our experiments show that user identification accuracy in this case rises to 97.5% using combination of audio and acceleration based features.

VI. DEMONSTRATOR

We have developed a demonstrator based on the proposed methodology for Apple iPhone mobile device. The demonstrator can detect an unexpected situation involving a free fall, impact and a period of no activity. Upon detection of such a risky unexpected situation, the demonstrator can automatically block access to the phone and ask for a password. It can also optionally send a message including the location of the mobile phone to a designated number.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented our initial investigations on the correlation between motion and audio information captured using embedded sensors in a mobile device for enhancing security functionalities related to the device. We have mainly investigated two cases. In the first case, we detect unexpected events, based on audio and movement analysis. We showed that an unexpected event such as a phone fallen down and left unattended can be identified with a high accuracy. For the second case, we proposed implicit user identification/authentication based on audio and movement analysis during regular physical activities (e.g., walking). We showed that a user can be identified with high accuracy on this basis. The results of such analysis can be used to arrange a graded security scheme for mobile and handheld devices based on their actual status. The proposed framework can be used as a stand-alone implicit security enhancement technique, or used as a complement to regular user authentication techniques. These results can be an initiation for a new security paradigm for enhancing security functionalities in mobile devices based on audio and movement analysis.

This work can be further developed by extending investigations for finding a general model describing the correlation between movements of a mobile device as well as ambient audio, with security risks. There are many other factors such as where the device is carried (e.g., bag, pocket, etc.) which can be also highly correlated with security of data and services on the device. Our proposed method can be also used for automatic profile management when a mobile device is shared between several users.

TABLE II. USER IDENTIFICATION RESULTS USING DIFFERENT FEATURE SETS(MOVEMENT, AUDIO, MOVEMENT+AUDIO)

Feature source	Accuracy
Movement	88.3
Audio	47.8
Movement + Audio	**90.1**

TABLE III. USER AUTHENTICATION MEASURES FOR SOME USERS

User ID	Precision	Recall	F-measure	ROC Area
1	0.89	0.95	0.92	0.98
2	0.92	0.87	0.90	0.96
3	0.92	0.91	0.92	0.98
4	0.92	0.92	0.92	0.97
Weighted Average	**0.91**	**0.91**	**0.91**	**0.97**

REFERENCES

[1] Improving Mobile Authentication http://searchmobilecomputing.techtarget.com/tip/Mobile-device-security-Improving-mobile-authentication, retrieved 12/12/2010.

[2] P. Gupta, S. Ravi, A. Raghunathan, and N. K. Jha, "Efficient Fingerprint-Based User Authentication for Embedded Systems," Design Automation Conf., pp. 244-247, June 2005.

[3] N. Aaraj, S. Ravi, A. Raghunathan, and N. K. Jha, "Architectures for Efficient Face Authentication in Embedded Systems," Proc. Design, Automation & Test in Europe, pp. 1-6, 2006.

[4] C. C. Leung, Y. S. Moon, and H. Meng, "A Pruning Approach for GMM-Based Speaker Verification in Mobile Embedded Systems," Lecture Notes in Computer Science, pp. 607-613, 2004.

[5] A. Yazji, X. Chen, R. P. Dick, and P. Scheuermann, "Implicit User Re-Authentication for Mobile Devices," Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing, pp. 325-339, Brisbane, 2009.

[6] J. Rekimoto, "Gesturewrist and gesturepad: Unobtrusive wearable interaction devices," In Proceedings of Fifth International Symposium on Wearable Computers, 2001.

[7] J. Rekimoto, "Tilting Operations for Small Screen Interfaces," UIST'96, pp. 167-168.

[8] K. Hinckley, J. Pierce, and E. Horvitz, "Sensing Techniques for Mobile Interaction," In Proceedings of ACMUIST, pp. 91-100, 2000

[9] H. Ketabdar, "Detecting physical shock by a mobile phone and its applications in security and emergency," Proceedings of MobileHCI 2009, Bonn, Germany.

 ISBN: 978-1-61208-117-5