An Evaluation of Behavioural Profiling on Mobile Devices

Fudong Li[1], Ross Wheeler[1], and Nathan Clarke[1,2]

[1] Centre for Security, Communications and Network Research (CSCAN), Plymouth University, Portland Square, Plymouth, PL4 8AA, United Kingdom
[2] Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia
{fudong.li,N.Clarke}@plymouth.ac.uk,
ross.wheeler2@students.plymouth.ac.uk

Abstract. With more than 6.3 billion subscribers around the world, mobile devices play a significant role in people's daily life. People rely upon them to carry out a wide variety of tasks, such as accessing emails, shopping online, micro-payments and e-banking. It is therefore essential to protect the sensitive information that is stored on the device against misuse. The majority of these mobile devices are still dependent upon passwords and Personal Identification Numbers (PIN) as a form of user authentication. However, the weakness of these point-of-entry techniques is well documented. Furthermore, current point-of-entry authentication will only serve to provide a one-off authentication decision with the time between an authentication and access control decision effectively becoming independent. Through transparent authentication, identity verification can be performed continuously; thereby more closely associating the authentication and access control decisions. The challenge is in providing an effective solution to the trade-off between effective security and usability.

With the purpose of providing enhanced security, this paper describes a behavioural profiling framework, which utilizes application or service usage to verify individuals in a continuous manner. In order to examine the effectiveness a series of simulations were conducted by utilising real users' mobile applications usage. The dataset contains 76 users' application activities over a four-week period, including 30,428 log entries for 103 unique applications (e.g. telephone, text message and web surfing). The simulations results show that the framework achieved a False Rejection Rate (FRR) of 12.91% and a False Acceptant Rate (FAR) of 4.17%. In contrast with point of entry approaches, the behavioural profiling technique provides a significant improvement in both device security and user convenience. An end-user trial was undertaken to assist in investigating the perceptions surrounding the concept of behavioural profiling technique – an approach that is conceptually associated with privacy concerns. The survey revealed that participants were strongly in favour (71%) of using the behavioural approach as a supplement of the point-of-entry technique to protect their devices. The results also provided an interesting insight into the perceived privacy issues with the approach, with 38% of the participants stating they do not care about their personal information being recorded.

Keywords: behavioural profiling, authentication, non-intrusive, transparent.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 330–339, 2014.

1 Introduction

With more than 6.8 billion subscribers around the world, mobile devices certainly play a significant role in people's daily life (ITU, 2014). Indeed, people rely upon them to carry out a wide variety of tasks, such as accessing emails, shopping online, micro-payments and transferring money via e-banking. These activities are inevitably associated with a certain level of personal and/or business information, such as corporate email, customer data, bank account numbers and personal contact details (Lazou and Weir, 2011; Checkpoint, 2013). Therefore, it is essential to protect the sensitive information that is stored on the device against threats such as when it is lost or stolen, infected by a virus or attacked using social engineering.

With the aim of protecting these mobile devices from user misuse, two forms of authentication techniques (i.e. Personal Identification Number (PIN) and biometrics) can be utilised. Currently, the majority of mobile devices are dependent upon the PIN as the first line of defence against unauthorised usage. However, the weakness of the PIN is well documented in the literature (Clarke and Furnell, 2005; Kurkovsky and Syta, 2010; Huth et al, 2012). For example, PINs can be poorly chosen, written down on a paper, shared with others or never changed. Biometric authentication is an automatic process to uniquely identify individuals based upon their physical (e.g. face) or behavioural (e.g. keystroke) characteristics and traits (Prabhakar et al, 2003). Recently, biometrics have begun to gain attention in the area of mobile authentication due to its ease of use. Indeed, a number of physiological biometric techniques have already been commercially implemented on mobile devices as an alternative security control, such as the Touch ID on the iPhone 5S and FaceLock on Google Android (Apple Inc., 2014; FaceLock, 2014).

As the existing PIN and biometrics techniques are implemented as a point-of-entry approach on mobile devices, they will only serve to provide a one-off authentication decision where the time between an authentication and a subsequent access control decision effectively becoming independent. Through transparent authentication, identity verification can be performed continuously; thereby more closely associating the authentication and access control decisions. The challenge in providing an effective solution is determining an optimal level between effective security and usability. To this end, this paper presents a novel behavioural profiling framework that provides continuous and transparent authentication for mobile devices, an experiment to underpin its capabilities and an evaluation of the technique based upon end users.

The remainder of the paper is structured in the following manner: Section 2 provides an insight into the current state of the art; Section 3 and 4 present the behavioural profiling framework and a preliminary evaluation of the framework through real user's application activities respectively. Based upon the promising simulation result, Section 5 presents the development of a prototype (called Sentinel). An end-user evaluation of the behavioural profiling approach is discussed in section 6. The paper concludes by highlighting future research directions.

2 Transparent Authentication on Mobile Devices

The concept of transparent authentication has become an area of active research since the turn of the millennium; however, with the significant enhancement of mobile device functionality, it has grown significantly in recent years (Clarke and Furnell, 2006; Clarke and Mekala, 2007; DARPA, 2011). It is also commonly referred to as continuous or active authentication. There are a number of authentication approaches that lend themselves to transparent authentication, such as behavioural profiling, keystroke analysis, facial recognition, speaker verification, gait and handwriting (Li et al, 2013; Clarke and Furnell, 2006; Weinstein et al 2002; Woo et al, 2006; Derawi et al, 2010; Clarke and Mekala, 2007).

Whilst much research has been undertaken in some biometric approaches, the transparent nature of the authentication approach requires further research – achieving point-of-entry authentication represents a significantly different problem to performing it transparently. Typically, variables that tend to be fixed in a point-of-entry scenario are not in a transparent mode of operation. For example, facial recognition would typically operate within an environment with fixed illumination with a facial image that is a fixed distance from the camera, with a fixed orientation. Within a transparent environment none of these aspects can be fixed – requiring a more flexible yet still secure approach.

As shown in Table 1, research is being undertaken to develop transparent biometric approaches and their performance is within the expectations of traditional behavioural-based biometrics in terms of Equal Error Rate (EER).

Table 1. The performance comparison of behavioural techniques on mobile devices

Behavioural Techniques	**EER (%)**
Behaviour profiling (Li et al, 2013)	10
Gait recognition (Derawi et al, 2010)	20.1
Keystroke analysis (Clarke and Furnell, 2006)	13
Handwriting recognition (Clarke and Mekala, 2007)	1
Speaker verification (Woo et al, 2006)	7.8

It is the purpose of this paper to focus upon and extend the current state of the art within one such area, behavioural profiling.

3 A Behavioural Profiling Framework

Based upon the foundation laid by the Transparent Authentication System (TAS) that utilises a mixture of biometric techniques to verify a mobile user's identity in a continuous and transparent manner (Clarke, 2011), the behavioural profiling framework was initially proposed by Li et al (2013). By employing the behavioural profiling technique as the authentication method, the framework is designed to work in the following style: verifies the user via their app usage in a continuous manner and

ensures the verification process is carried out in a user-friendly way (i.e. the user is mainly verified transparently). The framework can operate in one of the following modes: as a standalone security control, within an Intrusion Detection System (IDS) or within a TAS. A number of components have been devised to fulfil the purpose of the behavioural profiling framework (as illustrated in Figure 1). Details of them are described in the following sections.

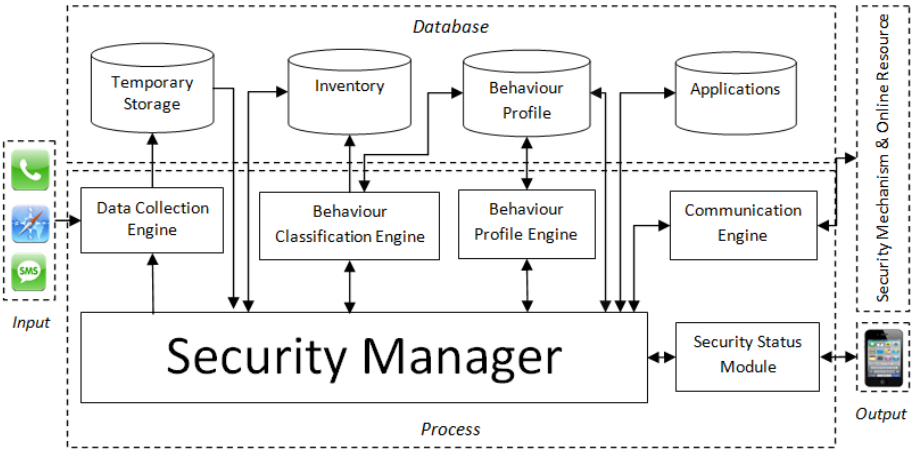

Fig. 1. A behavioural profiling framework (Li et al, 2013)

The Data Collection Engine is designed for capturing user's apps activities. It automatically collects various app features when an app is utilised. The Behaviour Profile Engine is used for the generation of various templates via the combination of user's historical data, a dynamic profiling technique and a smoothing function. With the aim of maintaining the accuracy of the templates, the dynamic profiling technique updates user's profile on a daily basis. The Behaviour Classification Engine performs the verification process whenever is required.

The Security Status Module is utilised to indicate how secure the system is. The framework can provide or deny access to the user when the system is at high or low security respectively. The security level of the system is calculated based upon the verification result and the quality of the sample being used. The quality factor is dynamically allocated to each app based upon their uniqueness (i.e. a higher factor is given to the app which is more unique/discriminative to the user). After the activity of an app is verified, the security level is increased (verified successfully) or decreased (verified unsuccessfully) by the performance factor of the app.

The Security Manager is central node of the framework as it co-operates with other components to complete various tasks, such as continuous verification and automatic profile updates. Among these tasks, the key responsibility of the Security Manager is to maintain the security level and make subsequent decisions when the user requests access to an app; this can be achieved by employing the System Security Status Monitor And Response (SMAR) algorithm that is designed to provide a high level of

user convenience and improved security (Li et al, 2013). The algorithm employs both transparent and intrusive methods to verify a user, with three main checking stages before the user is locked out by the device. Hence, it is envisaged that legitimate users will mainly experience transparent phases and intrusive challenges will only be utilised to ensure a user's legitimacy when access to the device is requested but the security level is below the requirement.

4 Empirical Simulation

With the aim of evaluating the performance of the framework, a simulation process was conducted. The simulation utilised a subset of the Massachusetts Institute of Technology Reality Mining dataset as its simulating data (Eagle et al, 2009). The subset contains 76 users' 103-app activities during the period of 24/10/2004-20/11/2004 as illustrated in Table 2. Each user's data was divided into two halves, containing first and second two-week activities respectively. A user's profile was initially obtained by using their first two-week activities; the profile was then dynamically updated on a daily basis. The rest of users' activities were employed to evaluate the performance of the behaviour profiling framework.

Table 2. The simulation dataset

	Normal Apps	**Telephony**	**SMS**
Users	76	71	22
Unique apps / telephone numbers	101	2,317	258
Logs	30,428	13,599	1,381

In order to evaluate the effectiveness of the Behaviour Profiling framework, the PIN based technique was chosen as a baseline method. Therefore, the framework was configured to verify a user's identity as soon as an app is utilised, similarly to the way how the PIN functions. Based upon this configuration, all users' activities were put through the framework.

With the aim of maximising the security, it is assumed that a PIN is required after the device has been idle for more than one minute. By utilising this setting, users are required to enter a PIN for every single app usage (i.e. no transparent authentication at all) if the PIN based technique was applied to the same simulation data. In comparison, the simulation result shows that the Behaviour Profiling framework achieved an overall FRR of 12.91%, indicating 87.09% of the time legitimate user will be transparently verified and automatically obtain access to the device. With the same configuration, the imposter has only a 4.17% opportunity to abuse an app and conversely 95.83% of the time they will be denied access. Based upon the above discussion, it demonstrates that the Behaviour Profiling framework is capable of

offering continuous and transparent security for majority of the time and is able to do so in a more secure and user convenient fashion. Nonetheless, the Behaviour Profiling framework should have a small footprint upon the device, permitting it to be possibly adopted by users. With this aim, a prototype of the framework is described in the following section.

5 Sentinel – A Prototype of the Behaviour Profiling Framework

Based upon the encouraging simulation results, a working prototype of the Behaviour Profiling framework, Sentinel, was developed to demonstrate the concept of the behavioural profiling technique on a real mobile device. Sentinel, designed specially to have a small memory footprint, is capable of monitoring user's app activities and then identifying the legitimacy of the actions accordingly.

A Google Nexus smartphone with Android 4.0 was chosen as the development platform because the open source nature of the operating system provides a flexible environment and also the large amount of market share of the Android presents huge number of potential users for the prototype (IDC, 2013). As the Behaviour Profiling framework utilises user's app activities to identify individuals, the initial barrier of implementing the Sentinel was whether the prototype can collect features of each apps. This was achieved by the support of several Android API classes as demonstrated in Table 3. As a result, Sentinel is able to collect various features of the app, such as time of usage, name of the app, the location of usage. Sentinel utilises the SQLite as its database to store user's app activities. All users' app activities are stored in the SQLite database initially until enough data is collected for building the user's behavioural profile. By utilising the user's profile and a dynamic rule-based classifier (Li et al, 2013), Sentinel can determine the legitimacy of each user's app activity and deal the classification result accordingly.

Table 3. Android API class for data collection process of the Sentinel

Android API class	**Description**
Activity Manager	Interacts with overall activities running on a device
Telephony Manager	Accesses telephony data relating to cellular location
Location Manager	Accesses location data relating to geo-location
Broadcast Receiver	Listens for outgoing call state changes
Phone State Listener	Monitors for incoming call state changes

Once the development of the Sentinel backbone was completed, a graphical user interface was also designed and developed, permitting user to perform various tasks. As illustrated by Figure 2, user can start the Sentinel by clicking on the "Start Service" button, browse various log files (e.g. an overview of user's app activities is presented by the Application Logs function) and review the classification results (i.e. 0 and 1 indicate unsuccessful and successful verifications respectively).

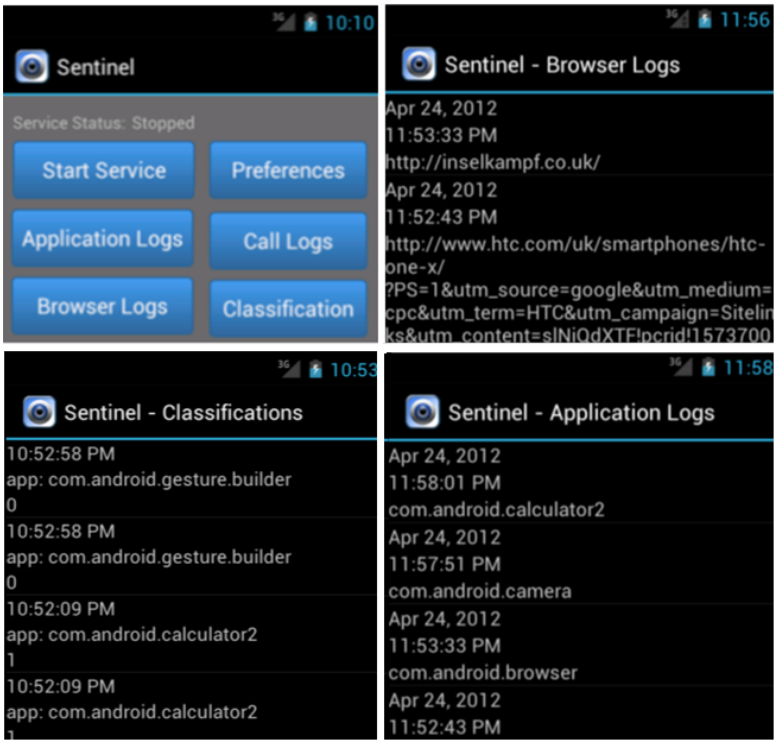

Fig. 2. A selection of screenshots of Sentinel

As demonstrated above, the prototype of the Behaviour Profiling framework, can identify user's identity based upon their apps usage. In addition, the user will not notice its existence because it not only mainly runs as a background service but also has a tiny footprint (i.e. 6KB) on the device's overall memory as illustrated in Table 4.

Table 4. An overview of Sentinel's memory

Services	**Memory**
Logging Service	4.9KB
Sentinel Activity	896B
State Listener	80B
Outcall Receiver	64B
Reminder	96B
Total	**6KB**

6 Evaluation of Behavioural Profiling on Mobile Devices

As user acceptance is crucial to the adoption of new technologies and processes, a survey was designed to obtain end-user perceptions on the behavioural profiling

technology. The survey contains 9 questions, covering participants' background of Information Technology (IT), how they utilise and secure their devices, and their opinion upon the behavioural profiling technique. As the behavioural profiling is a novel authentication technique, a brief description of its working principle was also provided to assist participants to understand how the technique provides transparent and continuous protection for mobile devices. The survey was conducted over the Internet and advertised through the use of social networking and word of mouth.

In total 55 participants completed the survey. The results shows that the participants have a wide range of technical experience with 9.1% classifying themselves with the beginner knowledge of IT category, 56.4% with intermediate knowledge and 32.7% with advanced or greater knowledge of IT systems. As illustrated in Figure 3, participants utilise several operating systems on their mobile phones: Android, iOS, Symbian, BlackBerry and Windows with 44%, 23%, 5%, 4% and 4% of users respectively. Despite 80% of the participants utilised smartphones, the SMS and telephony functions still remain as the most frequent used apps with 45% and 24% of the users accordingly, followed by email and internet browsing with 16% and 9% of the participants respectively.

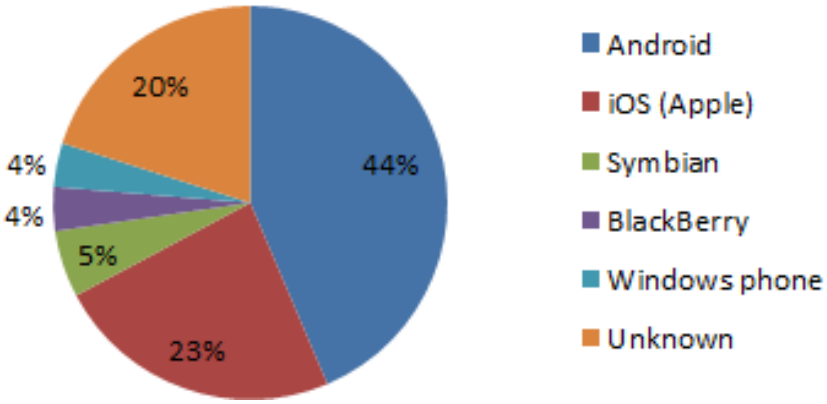

Fig. 3. Comparison of participants' mobile device operating systems

The survey also revealed that only 56.4% of the participants utilised the point-of-entry technique (e.g. PIN) and 54.5% of the participants believe they store important information (e.g. email messages and personal contacts) on their mobile devices. It all likelihood a far larger proportion of users have sensitive data but merely do not recognise it. Interestingly, 62% of the participants stated they do care about their personal information being recorded, revealing that privacy concerns may not be as great as literature suggests. The majority of participants were strongly in favour (71%) of using the behavioural approach as a supplement of the point-of-entry technique to protect their devices. For those who were reluctant in adopting the behavioural profiling technique, privacy was their primary concern (as illustrated in Figure 4).

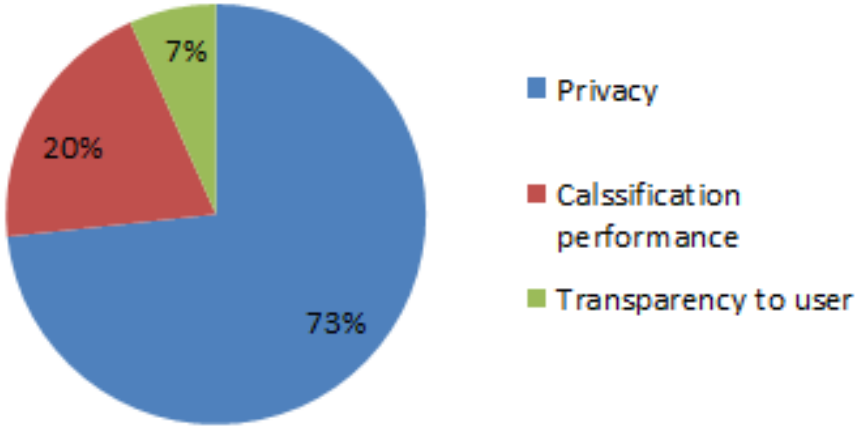

Fig. 4. Reasons for not adopting the behavioural profiling technique

7 Conclusion

The first part of the paper identified that authentication is an essential service that underpins the security of systems; however, current solutions fail to take appropriate consideration of the human-factors of good security design. Through behavioural profiling, transparent and continuous authentication provides the opportunity to overcome the systematic usability issues that exist offering an acceptable, more robust and more secure approach.

Based upon the promising simulation result, a proof of concept and end-user evaluation, the approach has demonstrated significant merit. However, care, particularly on issues of privacy need to be taken in consideration. In the future, a most robust and comprehensive version of the Sentinel should be developed with built-in privacy protection. This will also allow for a complete and longitudinal end user trial to be conducted.

References

1. Apple Inc., iPhone 5s: Using the touch ID kb/HT5883 (2014), http://support.apple.com/ (accessed: January 09, 2014)
2. Checkpoint, The impact of mobile devices on information security (2013), http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf (accessed: January 05, 2014)
3. Clarke, N.: Transparent User Authentication. Springer, Berlin (2011)
4. Clarke, N.L., Furnell, S.M.: Authentication of users on mobile telephones—a survey of attitudes and practices. Computer Security 24(7), 519–527 (2005)
5. Clarke, N.L., Mekala, A.R.: The application of signature recognition to trans-parent handwriting verification for mobile devices. Information Management & Computer Security 15(3), 214–225 (2007)

6. Clarke, N.L., Furnell, S.M.: Authenticating Mobile Phone Users Using Keystroke Analysis. International Journal of Information Security, 1–14 (2006) ISSN:1615-5262
7. DARPA, Active Authentication, DARPA (2011), http://www.darpa.mil/OurWork/I2O/Programs/Active Authentication.aspx (accessed: January 17, 2014)
8. Derawi, M.O., Nickel, C., Bours, P., Busch, C.: Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. In: Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (2010)
9. Eagle, N., Pentland, A., Lazer, D.: Inferring social network structure using mobile phone data. Proceedings of the National Academy of Sciences (PNAS) 106, 15274–15278 (2009)
10. FaceLock (2014), http://www.facelock.mobi/ (date accessed: January 08, 2014)
11. Gartner, Gartner Says Mobile App Stores Will See Annual Downloads Reach 102 Billion in 2013 (2013), http://www.gartner.com/newsroom/id/2592315 (accessed: October 10, 2014)
12. Huth, A., Orlando, M., Pesante, L.: Password Security, Protection, and Management (2012), https://www.uscert.gov/sites/default/files/publications/PasswordMgmt2012.pdf (accessed: January 09, 2014)
13. IDC, Android Pushes Past 80% Market Share While Windows Phone Shipments Leap 156.0% Year Over Year in the Third Quarter (2013), http://www.idc.com/getdoc.jsp?con-tainerId=prUS24442013 (accessed: January 23, 2014)
14. ITU, Global ICT developments (2014), http://www.itu.int/en/ITUD/Statistics/Pages/stat/default.aspx (accessed: January 06, 2014)
15. Kurkovsky, S., Syta, E.: Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In: Proceedings of the IEEE International Symposium on Technology and Society (ISTAS), pp. 441–449 (2010)
16. Lazou, A., Weir, G.: Perceived risk and sensitive data on mobile devices. Cyberforensics. University of Strathclyde, Glasgow, pp. 183–196 (2011) ISBN 9780947649784
17. Li, F., Clarke, N.L., Papadaki, M., Dowland, P.S.: Active authentication for mobile devices utilising behaviour profiling. International Journal of Information Security (2013), doi:10.1007/s10207-013-0209-6
18. Portioresearch, Fast growth of apps user base in booming Asia Pacific market (2013), http://www.portioresearch.com/en/blog/2013/fast-growth-of-apps-user-base-in-booming-asia-pacific-market.aspx (accessed January 10, 2014)
19. Prabhakar, S., Pankanti, S., Jain, A.K.: Biometric recognition: security and privacy concerns. IEEE Security & Privacy 1(2), 33–42 (2003)
20. Weinstein, E., Ho, P., Heisele, B., Poggio, T., Steele, K., Agarwal, A.: Handheld face identification technology in a pervasive computing environment. In: Pervasive 2002, Zurich, Switzerland, pp. 48–54 (2002)
21. Woo, R., Park, A., Hazen, T.: The MIT Mobile Device Speaker Verification Corpus: Data collection and preliminary experiments. In: Proceeding of Odyssey, The Speaker & Language Recognition Workshop, San Juan, Puerto Rico (June 2006)