User Authentication for Mobile Devices

Marcin Rogowski, Khalid Saeed, Mariusz Rybnik, Marek Tabedzki, Marcin Adamski

User Authentication for Mobile Devices

Marcin Rogowski[1], Khalid Saeed[2], Mariusz Rybnik[3],
Marek Tabedzki[4], and Marcin Adamski[4]

[1] King Abdullah University of Science and Technology,
Thuwal, Kingdom of Saudi Arabia
marcin.rogowski@kaust.edu.sa
[2] Faculty of Physics and Applied Computer Science,
AGH University of Science and Technology, Cracow, Poland
saeed@agh.edu.pl
[3] University of Bialystok, Bialystok, Poland
mariuszrybnik@wp.pl
[4] Faculty of Computer Science,
Bialystok University of Technology, Bialystok, Poland
{m.tabedzki, m.adamski}@pb.edu.pl

Abstract. The paper is intended as a short review of user authentication problem for mobile devices. The emphasis is put on smartphones and tablets, that nowadays are very similar to miniaturized personal computers with much more sensors of various origin. The sensors are described with remarks on their usefulness for user authentication. Deficiencies of traditional user authentication methods based on knowledge are pointed out and the need for new – more secure but also comfortable – user authentication mechanisms is reasoned. Preliminary user authentication systems employing biometric features are discussed and hence the generally unused potential of biometrics for mobile devices is demonstrated.

Keywords: user authentication, biometrics, mobile devices, touchscreen

1 Introduction

Mobile devices are constantly getting more popular and resourceful.

Nowadays they serve purposes of: personal information managing, various modes of communication, web browsing, documents editing, media presentation, etc., therefore largely replacing desktop computers. They contain large amounts of personal data and passwords. In 2005, even before the smartphone revolution had started, it was estimated that over 80 percent of new critical data is stored on mobile devices [1]. Increasingly, especially in post-2007 era, very similar services and applications are used on mobile devices and personal computers. Whilst security barriers were implemented on PC's for many years, it is a relatively new trend on the mobile devices. The need of securing aforementioned hundreds of millions of devices is obvious, with unauthorized access being the most common threat. The threat is countered by *user authentication*, being also the most

important user-dependent issue (hardware and operating system security being rather a matter of device developer than user).

The mobility results in high risk in comparison to desktop computers. Obviously, the chance of an attempted unauthorized access is higher when the device is carried and used in public. Few methods of securing mobile device do exist, PIN (a kind of password) being the most common. The methods mainly secure devices from unauthorized access when mobile device is unattended by the legitimate user.

Certainly one cause of the deficiencies of user authentication for mobile devices is the expected access time. In case of PCs, usually the user authenticates and then uses the machine for an extended time, so she is more likely to accept more sophisticated and cumbersome security check. For mobile devices, usually the user accesses the device often and for short periods of time, what makes a trustworthy user authentication less desirable, assuming it requires some effort. The time required to authenticate should be taken into account and – for the comfort and cooperation of the user – be minimized.

The paper is organized as follows: section 2 presents the data sources available from mobile devices' sensors, section 3 discuses user authentication methods. Due to space limitation, the paper shows only the most striking-out approaches, that are especially interesting taking into account mobile devices functions and specifics. Finally the last section summarizes the paper and gives further predictions on the mobile market development.

2 Sensors of Mobile Devices

Mobile devices are currently equipped with many sensors that provide much more data than traditional communication channels of desktop computer – keyboard, mouse and screen. The key difference in the interaction with mobile devices and desktop computers is the interface. We rarely see a physical keyboard and almost never see a mouse attached to a mobile device. Most of the time touchscreens are used to interact with the device and replace both mouse and keyboard, with virtual keyboard displayed on the screen and typed using the display embedded in the device. This is the most important technology advance, that combine means of outputting visual data with inputting both: discrete data (characters and GUI interaction) and spacial data (touching, swiping, gestures at the specific coordinates).

Touchscreen provides more features than traditional interaction with a desktop computer. Physical keyboard is replaced by a virtual one and in addition to timing of keystrokes, also the size of each finger pressing a screen can be measured, pressure is estimated and the exact position of the finger pressing a key in relation to the position of this particular key pressed can be analyzed. In contrast to a PC, mobile devices – whether tablets or phones – produced these days, also have a plethora of other sensors most often including: an accelerometer, a gyroscope, a proximity sensor, an ambient light sensor, two microphones, one or two cameras and sometimes even a magnetometer. Some of these sensors

obviously can provide more information about the user and his behavior and help differentiate between users. Table 1 presents the most important sensors, along with a quick remarks on their usefulness for user authorization.

Table 1. Sensors of mobile devices

Sensor	**Remarks**
Physical keyboard	usually no pressure control and no dwell registering
Touchscreen	exact coordinates and "touch size" may be used as information
Microphones	usually two microphones, one for user voice and the other for noise-canceling
Camera	High quality image (8 Mpix and more)
Video camera	High quality video (for example HD quality)
Accelerometers	usable in gait dynamics [2] or in multi-biometric authentication
Gyroscope	not directly applicable to user authentication
Proximity sensor	usually detects only presence of nearest object (binary information)
Ambient light sensor	environment lightness, not directly applicable to user authentication
GPS	not applicable to user authentication
Compass	not applicable to user authentication

What is important, most of the data coming from the aforementioned sensors can be collected transparently to the user. That creates two possibilities: either to use it alongside the traditional methods discussed before (that is to strengthen the password rather than replace it) or to continuously authenticate the user. In the second approach, data is collected and analyzed all the time as the user ordinarily uses the device. With such *background authentication system*, even if the device is stolen in the authenticated state (for example grabbed from the users hand), an algorithm analyzing particular data may determine that the user using the device is no longer the legitimate one and may block the device.

3 User Authentication for Mobile Devices

Most of the user authentication methods may be adopted for mobile devices. Also, due to mainly instantaneous access time expected by the user, they do not seem to work very well because they are used in less secure versions.

Few of available sensors are widely involved to authenticate users of mobile devices. Mostly conventional security precautions are used, even when some sensors can enhance the existing methods and provide raised level of security. Many of the discussed characteristics do not require user cooperation (or even their knowledge) and can be collected in the background. That allows creation of a system that will continuously authenticate the user, based on his actions, without harassing the legitimate user. The goal of such system would be to block

access to the device immediately after detection of suspicious behaviour. This may not only prevent an unauthorized access to the device when it is stolen in authorized state, but would also make compromising or breaking the password using brute-force methods virtually impossible.

Commonly PCs are shared by more than one person, contrastingly, mobile devices are almost never shared. This fact encourages to use biometric features for user authentication. It should also be noted that as any password, a biometric password can sometimes be lost. Certainly unpleasant situations as losing ones physical feature like a fingerprint might happen and despite being unlikely, some backup method of authentication should be thought of.

Following sections will discuss different user authentication methods, grouped into knowledge based methods and biometric methods, as token-based methods for mobile devices are virtually non-existent.

3.1 Knowledge based methods

Knowledge based methods are based on exclusive user knowledge of some sort. Passwords, PINs, pattern locks and graphic passwords are based on user memory, therefore unfortunately require some effort and are very prone to forgetting.

Password The most popular desktop securing method – a password – is also ported in the same form to mobile devices. This however, is not as acceptable by the users as for desktop computers. A mobile device user expects almost instant access, and it is unlikely, that the user will voluntarily sacrifice convenience for security. Many will easily agree for a minor discomfort of a few seconds of delay, but it is unlikely that they would agree to a password as difficult as the passwords we use nowadays on desktop computers.

There are some publications describing what characterizes a good password – e.g. *complexity*, *uniqueness* and *secrecy* rules proposed in [3]. Unfortunately users most likely compromise one or more of these rules for their comfort. On a mobile device, designed to be comfortable, users are even most likely to jeopardize the *complexity* rule.

PIN – Personal Identification Number is a special case of a password, known well from ATM machines. In banking it dates back to 1966 when James Goodfellow patented a PIN derivation scheme [4]. Despite contemporary standards requiring its length to be 4–12 digits, most often used numbers are still of the length of 4 digits only. This carries a clear disadvantage as it can be easily calculated – there are only 10 000 possible PINs so the level of security proposed does not seem to be high. In banking, it is usually coupled with blocking the card after three failed attempts and hence some level of security is ensured – probability of guessing a PIN within three attempts is only 0.06%. It also still remains relatively comfortable for the legitimate user.

PIN was also adopted by smartphone makers as a security measure. The length is no longer fixed to 4 with the newest Android system specifying the

length of a PIN to be between 4 and 17 characters. Apple still uses the length of 4 for iPhone and iPad but Simple passcode mode may be turned off changing a PIN into a password, as discussed before. Regrettably, there should be no illusion that mobile users will actually use a long number. Most likely the biggest group will use 4 digits and many of those will be birth dates, patterns on keyboard or common passwords like 1234. Recent study has clearly shown these tendencies [5]. After analyzing 204 508 PINs from iPhones it turned out that 46 of the possible combinations were not even used and 4.3% of all the PINs were 1234. Another problem with the use of a PIN on a mobile device is that it would not be acceptable, as in banking, to cause major discomfort for a user after he or she inputs a wrong number three times. The number can be entered numerous times during a day on a mobile phone, so mistakes, even many times in a row may happen. The solution used now by Android developers is locking the device for a predetermined period of time so it protects the device from spontaneous brute-force attacks when it is unattended for a few minutes. However, this simple lock is not going to protect the device if it can be accessed for a longer period of time. Apple included an option to erase all the data on the phone after the PIN is entered incorrectly for 10 times, but this solution may frustrate users, especially if they have kids or if a user with malicious intent gets access to their device even for a few minutes.

Another problem is that the PIN encourages users to pick the numbers that create a pattern on a keyboard and makes the password predictable. In general, a PIN can be considered as a special case of password that carries all its deficiencies.

Pattern locks Another form of a security measure that can be used on contemporary touchscreen devices is a pattern lock. Instead of a PIN, the user is required to connect dots in a predefined order. Surely, that kind of pattern may be easier to memorize and does not cause major discomfort for the user.

The researchers from the University of Pennsylvania explored deficiencies of pattern locks in [6]. As calculated there, in general there are about 1 million possible patterns using 9 points. However, if constraints of implementations are taken into account – for Android, if a point lays between two selected points, it also has to be selected – there are only 389 112 combinations left. If the users comfort is also taken into account, it turns out, that more than a half of these combinations contain patterns that are not comfortable for the user to enter. As the users pick convenient patterns, it is not likely that they will pick one of these special cases and as a result search space can be narrowed down to 158410 likely combinations.

The discussed paper exposes another drawback of using pattern locks on touchscreen devices: oily residue left behind by finger. Using photo-editing software they were able to successfully expose the trace of a finger and in the report they state the method worked in 92% of the cases.

A solution to the problem was proposed by *Whisper Systems* with their product *Whisper Core* offering smudge-resistant screen unlock patterns [7]. The

solution proposed is to force the user to replace pattern-smudge with another smudge – namely wiping the entire screen with a finger. It is some solution to the problem but the problem with wider adaptation of the method may be again, the comfort of the user. This method adds at least two additional strokes of a thumb so for some users it may double the effort of unlocking a screen.

Another risk of using a pattern lock is that it is quite easy to be compromised. It is usually a characteristic pattern and it can be easily observed and memorized.

Graphic passwords Replacing PIN with a graphic password is another idea of using the nature of touchscreens to improve upon the security of the PIN. One of the ideas was introduced by J. Citty in [8]. Instead of using a 4-digit sequence, 16 images partitioned into four parts are used. To verify the user, they are required to select the correct parts of the correct images in the right order. This change increases the number of possible password combinations from 10^4 for a 4-digit PIN to over 10^7. The sequence entry time is initially about two times that of a PIN, but as users practise, it gets close to it.

3.2 Biometrics

When authenticating with a password, a PIN or a pattern, the authentication is a binary problem – either the predetermined pattern matches or it does not. When using biometric features, the problem is more complex. Whether it is a fingerprint, a face image or any other biometric feature, it is very unlikely that the obtained feature will exactly match the one collected whilst enrolling the user. There is always a tradeoff between False Acceptance Rate and False Rejection Rate. Minimizing FAR makes the system more secure but at the same time causes discomfort to the users by making FRR higher and vice versa.

Face recognition Face recognition is a very well known biometric feature analysis. Recently with development of hardware and processing power, it has been used with success in many environments [9].

Considering mobile devices applications at large: *Face Unlock* is a new feature added to Android system in late 2011. It is also the first biometric feature used there. It has to be admitted that this implementation of unlocking using face image works instantaneously. Unluckily, for this level of comfort, a price had to be paid.

Clearly, to achieve the speed and low "insult rate" as FRR may be called, developers of Android had to sacrifice FAR therefore making *Face Unlock* less secure. It is even incorporated as a standard warning to the user that *Face Unlock* is less secure than other methods and persons looking similar will be able to get access to the device. What is not mentioned is that also people having a picture of a person that looks similar to the user will be able to get access to the system as a simple camera will not be able to tell the difference between the actual face and the picture of the face being in front of it.

There are also a few different problems with *Face Unlock*. The environment lighting plays a big role and the method will simply not work when it is too dark or too bright. Another fact is that the position of the device when taking a picture is important, so it will not be possible to use this method to unlock a phone or a tablet lying flat on the desk or to do it discreetly in public without positioning a device in front of ones face. There is also a requirement for the device, as it has to be equipped with a front-facing camera to make it comfortable to use.

Keystroke dynamics The users typing style was shown to be a feature differentiating fairly well between users. The idea (for personal computers) first came as early as 1975 when it was mentioned by R. J. Spillane [10] and has since then been modified and improved on multiple occasions with the results reported as high as 99-100% correct classification. In general, in almost all the works on keystroke dynamics the user is asked to type a particular password multiple times.

The same characteristics that were used on a physical keyboard may be usually used on the touchscreen keyboard. Many more properties may be registered including exact location of finger on the virtual button, the size of touching finger, the pressure, and the changes in position coming from both the accelerometer and the gyroscope. This gives a huge potential for keystroke dynamics to be used for user authentication.

The same approaches as in traditional keystroke dynamics can be used – a fixed-text authentication and a free-text authentication. In the case of the fixed-text authentication, the user will perform the verification procedure as usual – whether it is a pattern lock, PIN or a password and not only correctness of the combination would be evaluated but also how they did it. There are a number of features that can be extracted to help determine if a user is a legitimate one. For traditional keystroke dynamics, the *dwell* time of a single key press is universally used. Most commonly it is combined with the so called *flight* time – time from releasing a key to pressing a subsequent one in the password. These characteristics proved to be reliable and there are no significant improvements over these results if additional features are extracted. It has to be considered if the problem is exactly the same on a small touch screen – usually around 4 inches in diameter for a phone and around 10 inches for a tablet – as on a full-sized physical keyboard.

Some preliminary research was done a few years ago on mobile phones when touchscreens were not prevalent in the market. A device with a small, thumb-typed physical keyboard was used by [11] and some interesting observations were made. In contrast to the full-sized physical keyboard, in this case, the dwell time of any single key did not prove to be a reliable differentiating characteristic and the resulting error rate was near 50%. Using the flight time between pairs of keys resulted in a much better 12.2% error rate on a group of 50 participants. The results obtained point out that the fact that the depression time of a key is not a good discriminating feature may be caused by the use of thumb-typed keyboard.

Initial research done on a device with 4.3 inch touchscreen shows that dwell and the flight times both give an error rate higher than 10% if not combined with additional features. The results obtained combining different characteristics, for example the dwell time and the size of the finger, are very promising but as the area is relatively new, comprehensive results are not yet available. Another interesting approach was evaluated for the full-sized physical keyboard [12], but may be relevant to mobile devices: free-text keystroke dynamics authentication running in the background and monitoring the user behavior. The motivation for this approach is the risk that an impostor gets the access to the computer when the user is logged in and will continue working as if he was authorized. Because of the very nature of mobile devices, this risk is amplified and, if implemented well, the continuous authentication approach may prove to be very relevant and useful in the new area.

In the case of a virtual keyboard displayed on the touchscreen, there is also the possibility to extract exact coordinates where the keys were pressed, the size of the users fingers that touch the screen and sometimes the pressure put on the display. Initial research has shown the finger size to be a very promising differentiating feature while the pressure, on physical keyboards, was shown to be as effective as latency information [13]. A huge advantage was clear when the latency and the pressure information were combined – accuracy was significantly improved.

Gestures Recently a study of biometric-rich gestures was conducted by a team led by Prof. Nasir Memon and published in [14]. The authors used tablets and asked users to perform particular gestures such as closing, opening, and various rotations, all in many different versions with different fingers fixed. The user-defined gesture was also allowed and in this case the movement of five fingertips while the user was signing his signature was recorded. In the verification phase, the input is compared to the stored template and based on the similarity, the user is authenticated or not. A Time Warping algorithm is used to compare the similarity of the two sequences. 34 users were asked to participate. From the predetermined methods, counter-clockwise rotation of all five fingers gave the best results with 7.21% Equal Error Rate, whilst the average was 10%. The researchers also evaluated the performance when two gestures were used. In this case the error rate was significantly lower and as low as 2.58% for clockwise rotation of five fingers followed by counter-clockwise rotation of four fingers with fixed thumb. This result indicates that different gestures make different characteristics of hand or the users interaction style stands out. The user-defined gesture was also very effective and the error rate was 2.88% in this case. It is important that most of the users said that the gestures are pleasant to use and a good number said they were *excited* to use them. 25 out of 29 users preferred this method over a text password and all 29 users thought it would be faster.

Touchscreen dynamics versus mouse dynamics Mouse dynamics is a method of evaluating the users specific style of moving a mouse. Different re-

searchers analyzed different characteristics, often including deviation from the straight line, a user-specific ratio of dragging, clicking, average speed etc.

On a touchscreen device, the users finger takes the role of the mouse. Similarly as in physical/virtual keyboard comparison, using a touchscreen provides all the same information and a few features more. Not only X and Y coordinates in time can be recorded, but additionally there is also the information about the size and the pressure. What may be important for some concepts, like gesture recognition, the most modern touchscreens support multi-touch, i.e. more than one finger interacting with the screen at the same time.

One of the interesting and relevant approaches was introduced in 2005 by Hashia et al. [15]. The teams system asks users to connect some dots. Dots are shown one at a time and the user is simply required to move the mouse from one dot to another. The coordinates of the mouse are recorded every 50ms and the speed, the deviation from a straight line and the angle are calculated. In the verification phase, these values are compared to the ones recorded during the enrollment phase. The resulting error rate is 15%, which is not that bad considering how simple the statistical model is. It is quite easy to notice the similarities between this method and the pattern lock used in Android phones. Authenticating using a pattern lock is basically the same task – connecting dots, but only the order in which the dots are connected is evaluated. It is a very simple extension to also include some statistical information about the speed, the angle or the deviation from a straight line, as in the work discussed, to the same system. The change will be transparent to the user but may result in increasing the security level.

Hashia et al. also discuss the continuous authentication introduced before or as they call it – passive authentication. Instead of requiring the user to move the mouse over dots, whole regions of screen are treated as dots. They record the movements, and every two minutes analyze them and authenticate the user. No detailed performance characteristics are provided but an average time of 2 minutes for which the intruder was allowed to use the computer and 5 minutes after which the actual user was considered an intruder which suggests that False Rejection Rate may be alarmingly high. Passive authentication could be implemented on a mobile touchscreen as well. Slightly different approach was evaluated in [16]. Only the speed of the mouse between pre-determined points was analyzed and using minimal eigenvalues of a Toeplitz matrix for classification resulted in accuracy of almost 70%. On a touchscreen, data about pressure and size of the fingers could also be used, giving more discriminative features and the result would be most likely improved.

Voice recognition There are two approaches to voice (speaker) recognition – text-dependent and text-independent. Both could be used on a mobile device, especially a phone. If the voice analyzed in background during the conversation does not match the pattern stored beforehand, an additional authentication may be triggered. This method will protect users from the impostors that managed to come into possession of the primary password.

The speaker recognition due to some inconveniences instead to be used standalone may be used for multi-biometric systems discussed later. The performance of text-dependent speaker recognition systems is estimated to be similar to those of signature at error rate of about 2% [17].

Enhanced pattern lock The authors in [18] proposed an approach to authenticate users on the basis of the correctness of the pattern they enter and the way they do it. This is a direct translation of keystroke dynamics enhanced password to a pattern lock. Similarly as in Memons work [14], a Dynamic Time Warping algorithm is used to compare the similarity between the reference and the current input. Here x-y coordinates, time, size, pressure and speed are collected. Based on the data set of 31 users, researchers have achieved 77% accuracy with 19% false rejection rate and 21% false acceptance rate. Modifying the threshold used for some of the users helped to further improve the accuracy. It also suggests, that machine learning approach can be evaluated for the same problem and it should be checked how its performance compares to simple thresholds based on the Dynamic Time Warping algorithm.

Gait analysis In [2] authors used the data from the mobile phone accelerometer to distinguish between users, basing on the way they walk (gait dynamics). The achieved equal error rate of 20.1% is higher than in other works on the subject, but only a standard mobile phone was used and not specialized equipment or video recording like in the other cases.

Multi-biometric authorisation Certainly the abundance of sensors providing various, also biometric data allows to create some kind of a system that will combine these inputs and authenticate the user based on the combination of features. One such system was proposed by the researchers from MIT in 2003 [19] using a personal digital assistant device with a resistive touchscreen but no phone option. Their system investigates the usage of two-way multi-biometric authentication combining the face image and the speaker recognition. The image of the face is taken using the embedded 640x480 resolution camera. For the speaker recognition a built-in microphone is used which registers users voice pattern when pronouncing a password consisting of three two-digit numbers. The results obtained are promising with the error rate below 1% when analyzing both the face and the voice.

As mentioned, the important factor is user comfort. Efficient enrollment is also important and it is unlikely that users will chose to replace their PINs and patterns with a multi-modal system which takes an average of 30 minutes to set up – MIT researchers required users to take 25 face images in different lighting settings and to recite 16 generated pass phrases.

4 Conclusions

Mobile devices are becoming ubiquitous but their specifics causes security issues. Security measures are frequently omitted by users for the sake of comfort. Unauthorised access or loss of mobile devices is costly, as increasing amount of personal data is stored on them. Biometric solutions are rare and mostly are only available as third party applications, therefore unknown or disregarded by large audition. *Face Unlock* introduced to Android in late 2011 is the first biometric security measure available in large scale.

Hardware sensors of mobile devices are numerous and much biometric data is available. Possible applications of the biometric data available on mobile devices were discussed. Some of the new methods already experimentally implemented are described, others pointed out as possible research directions. Relevant approaches on different hardware, like mouse dynamics, were reviewed to assess their usability on the new type of devices.

Hopefully, for the sake of security, new security measures employing biometric features – however maintaining the users comfort – will be widely adapted for mobile devices, eventually becoming largely available as an integral part of mobile operating systems.

Acknowledgement

This work was partially supported by AGH University of Science and Technology in Cracow, grant no. 11.11.220.01.

References

1. Allen M.: A day in the life of mobile data. Mobile Security, British Computer Society. http://www.bcs.org/server.php?show=conWebDoc.2774 (2005) Accessed 14 May 2012
2. Derawi, M.O., Nickel, C., Bours, P., Busch, C.: Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition. Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP) 306–311 doi:10.1109/IIHMSP.2010.83 (2010)
3. Burnett, M., Kleiman, D.: Perfect Passwords. Syngress, Rock-land, MA (2005)
4. Ivan, A., Goodfellow, J.: Improvements in or relating to Customer-Operated Dispensing Systems. UK Patent #GB1197183. doi:10.1049/el:19650200 (1966)
5. Bonneau, J., Preibusch, S., Anderson, R.: A birthday present every eleven wallets? The security of customer-chosen banking PINs. Financial Cryptography and Data Security. http://www.cl.cam.ac.uk/ jcb82/doc/BPA12-FC-banking_pin_security.pdf (2012) Accessed 14 May 2012
6. Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge Attacks on Smartphone Touch Screens. Workshop on Offensive Technology. http://static.usenix.org/event/woot10/tech/full_papers/Aviv.pdf (2010) Accessed 14 May 2012
7. Whisper Systems WhisperCore. http://whispersys.com/screenlock.html. Accessed 14 May 2012

8. Citty, J., Tapi, D.R.H.: Touch-screen authentication using partitioned images. Elon University Technical Report. http://facstaff.elon.edu/dhutchings/papers/citty2010tapi.pdf. (2010) Accessed 15 May 2012
9. Tolba, A. S., El-baz, A. H., El-harby, A. A.: Face Recognition: A Literature Review. International Journal of Signal Processing, vol. 2, no. 2, 88–103 (2006)
10. Spillane, R.: Keyboard Apparatus for Personal Identification. IBM Technical Disclosure Bulletin, vol. 17, no. 3346. doi: 10.1109/MSP.2004.89 (1975)
11. Karatzouni, S., Clarke, N.L.: Keystroke Analysis for Thumb-based Keyboards on Mobile Devices. In Proceedings of the 22nd IFIP International Information Security Conference (IFIP SEC 2007), Sandton, South Africa, 14-16 May, 253–263. doi: 10.1007/978-0-387-72367-9_22 (2007)
12. Rybnik, M., Tabędzki, M., Saeed, K.: A Keystroke Dynamics Based System for User Identification. In Proceedings of the 7th International Conference on Computer Information Systems and Industrial Management Applications: CISIM'08. IEEE Computer Society, 225–230. doi=10.1109/CISIM.2008.8 (2008)
13. Loy, C.C., Lim, C.P., Lai, W.K.: Pressure-based Typing Biometrics User Authentication Using The Fuzzy ARTMAP. Neural Network International Conference on Neural Information Processing. http://www.eecs.qmul.ac.uk/ ccloy/files/iconip_2005.pdf (2005) Accessed 14 May 2012
14. Sae-Bae, N., Ahmed, K., Isbister, K., Memon, N.: Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems (CHI '12). ACM, New York, NY, USA, 977–986. doi=10.1145/2207676.2208543 (2012)
15. Hashia, S., Pollet, C., Stamp, M., Hall, M.Q.: On Using Mouse Movements As a Biometric. In Proceedings of the International Conference on Computer Science and its Applications. http://www.cs.sjsu.edu/faculty/pollett/papers/shivanipaper.pdf (2005) Accessed 15 May 2012
16. Tabędzki, M., Saeed, K.: New Method to Test Mouse Movement Dynamics for Human Identification. KBIB 2005 conference, Tom I, Computer Science Telemedicine Systems, Czestochowa Technical University Press, Poland, 2005, 467–472 (in Polish). http://home.agh.edu.pl/ saeed/arts/2005%20KBIB.pdf (2005) Accessed 15 May 2012
17. Myers, L.: An Exploration of Voice Biometrics. GSEC Practical Assignment. http://www.sans.org/reading_room/whitepapers/authentication/exploration-voice-biometrics_1436. (2004) Accessed 15 May 2012
18. De Luca, A., Hang, A., Brudy, F., Lindner, C., Hussmann, H.: Touch me once and I know it's you!: implicit authentication based on touch screen patterns. In Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems (CHI '12). ACM, New York, NY, USA, 987–996. doi=10.1145/2207676.2208544 (2012)
19. Hazen, T.J., Weinstein, E., Park, A.: Towards robust person recognition on handheld devices using face and speaker identification technologies. In Proceedings of the 5th international conference on Multimodal interfaces (ICMI '03). ACM, New York, NY, USA, 289–292. doi=10.1145/958432.958485 (2003)