WALAILAK JOURNAL
http://wjst.wu.ac.th Minireview

A Survey on Smartphone Authentication

Suwimon VONGSINGTHONG[*] and Sirapat BOONKRONG

Faculty of Information Technology, King Mongkut's University of Technology North Bangkok, Bangsue, Bangkok 10800, Thailand

([*]Corresponding author's e-mail: suwimonv@yahoo.com)

Received: 24 September 2013, Revised: 14 November 2013, Accepted: 2 January 2014

Abstract

The growing use of smartphones is actuating the need for better protection. Practically, smartphone users are often not adequately alert when it comes to protection of their credentials stored in the phones, even if they are very much concerned about security, reliability and privacy. To efficiently reduce smartphone vulnerability, an appropriate authentication which does not create more of a burden to users is required. In consequence, the three novel authentication premises that are typically used to authenticate users: something you know, something you have, and something you are, are examined. The basics of smartphone architecture are introduced. The strengths and limitations of each technique are highlighted, while several comprehensive solutions have been presented to encourage smartphone users to understand the capabilities of their current systems. A discussion on real-world experience of those techniques is also proffered as an open challenge to magnify the aftermath.

Keywords: Authentication, security, smartphone, vulnerability

Introduction

Research indicates that around 80 % of humans across the globe own a mobile phone. Out of the 5 billion mobile phones owned, approximately 1.08 billion are smartphones [1]. Moreover, a survey conducted by GfK Retail and Technology Asia has indicated that almost 3 million smartphones were sold in just the first 4 months of 2013, and demand is particularly strong, with the sales forecast to be triple that of last year. Harmoniously, demand for smartphones in Thailand is soaring impelling Thailand to stand as the second biggest Southeast Asian smartphone market placed behind Indonesia [2]. Most of these devices, running iOS, Android, and other operating systems, offer the flexibility to install custom applications to be used for various purposes. As a result, mobile devices are used as primary devices for keeping track of meetings, appointments and for storing pictures and videos. The reason why personal and sensitive information would generally be stored on mobile devices [3] ascribable to roughly a quarter of mobile users mainly uses their mobile phones to go online and to access emails and social media [4]. As of their massively beneficial qualities, smartphone is thought of as a light version of computer with ubiquitous telephonic functionality.

Ready access to services is one of the factors which increasingly propelled smartphone to security threats. Without proper precautions, our own records or our own digital identities stored on these devices can be at immense risk. In our common lives, we are inevitability forced to adopt the process of positively verifying the identities of users, devices, or other entities, as a prerequisite to allowing access to resources on smartphones [5]. The process of verifying the validity of a claimed user can be more narrowly defined as authentication, where the trusted communications between authorized parties for computing and telecommunications applications can be accomplished by matching some short-form indicator of identity, such as a prearranged shared secret generated during enrollment or registration. To alleviate the anxiety of smartphone users with regard to the vulnerability to their precious information, this paper focuses on 2 facets of authentication: i) authentication on a smartphone, ii) using a smartphone to assist in authentication. The comparison of various approaches in terms of pros and cons of security, usability, handiness, and cost of smartphone are highlighted. Security measured by the hindrance to threats and usability indicated by the convenience to users are concurrently explored.

The remainder of this article is organized as follows: the second section discusses the architecture of smartphone, security-related factors, and its respective sensing capabilities. The third section investigates the up-to-date widely implemented techniques for authentication, as well as pointing out strengths and weaknesses. Finally, the last section emphasizes the advantages/limitations in terms of expedience, charges, security and risk assessment of each mechanism, to enable users to choose the most suitable authenticators for their devices.

Typical architecture of smartphones

Security related factors

The 3 major shifts in technology that should change the way we think about smartphone security are [6]:

1) Mobility. Mobility creates uncertainty about the environmental conditions surrounding smartphones. Devices may be used in secure environments or in public spaces. The variety of environments exposes mobile devices to a large pool of potential attackers: everyone from friends and family members to total strangers.

2) Sensors. Typical sensors found in modern smartphones are accelerometers, gyroscopes, magnetometers, proximity sensors, microphones, cameras, Global Positioning System (GPS), and radio (cellular, Bluetooth, Wi-Fi, RFID, NFC) antennas. These sensors fuel an explosion of new applications contoured for mobile devices, even though there are restrictions on ease of defined use, cost, and availability [7].

3) Constant connectivity. Constant connectivity allows devices to have constant access to the Internet and other devices, which can offload some security-relevant computations to remote servers or other machines.

Sensing

Sensors available on mobile phones can be classified as inertial, positioning, and ambient sensors. Each of these types of sensor is capable of sensing different aspects of user context, and are selected and configured based upon application requirements. Their sensing capabilities and current applications are introduced as follows [8]:

1) Inertial Sensors are sensors that are able to measure the physical motion of a solid object.

- Accelerometers are typically electromechanical instruments that measure the applied acceleration acting along their sensitive axis. The measured acceleration can be static, like the constant force of gravity, or dynamic, caused by moving or shaking the accelerometer.
- Gyroscopes are non-rotating sensors which basically use the Coriolis Effect on a mass to detect inertial angular rotation [9]. The embedded gyro sensors have been used in physical activity recognition [5] and body posture detection [10].

2) Positioning Sensors and User Proximity Detectors are capable of sensing the user's location and the presence of entities in their proximity. Apart from GPS, which is primarily used for outdoor positioning, Cellular, Wi-Fi, and Bluetooth signals are also used for user localization. The short-range communication link that can be provided by Bluetooth devices is also a very popular tool for probing a user's surroundings.

- Bluetooth and NFC are both short-range communication technologies integrated into mobile phones. The maximum working distance of NFC is less than 20 cm, while Bluetooth is approximately 100 m for class A and 50 m for low-energy Bluetooth [11].
- Cellular network based positioning uses trilateration techniques to calculate the current smartphone location. The cellular network is divided into cells, in which each cell has a unique identifier (cell-ID), and the cell size ranges between 50 m to a few kilometers. Each cell is interconnected with

other cells mostly through a wired backbone network. The maximum range of a cellular depends on a variety of factors, such as population density, the spacing of cell masts, and the terrain. Some technologies, such as GSM, normally have a fixed maximum range of 35 km; with CDMA and IDEN, it is possible to get between 50 and 70 km. The cellular network based positioning can calculate the location of smartphone very accurately due to the number of cell-sites surrounding it [12,13].

- GPS provides the position of the user nearly anywhere on earth. Nonetheless, the poor performance of GPS-based methods in indoor environments has energized the popularity of Wi-Fi.
- Wi-Fi is a means to provide wireless connectivity to devices that require quick installation or, in general, to mobile devices inside a wireless local area network (WLAN) [14]. A standard Wi-Fi might have a range of 35 m indoors and 100 m outdoors [5,11].

Among those, Wi-Fi and Bluetooth seem to be the most interesting choices if the barrier on cost and power consumption is diminished. In fact, wider adoption of Bluetooth, and advances in low energy technology, could eventually make Bluetooth a viable option. The most novel communication approach is RFID, which has a long range reading distance between 50 to 100 m [15]. It can indeed become the communication technology of choice for hardware authentication if barriers such as cost and the low availability of the reader in smartphone are solved.

3) Ambient Sensors are sensors that can be used for sensing the surroundings of a user, such as a camera, magnetometer, or microphone. A sensor network is mainly used for environmental monitoring purposes [16].

- Cameras are ubiquitous imaging devices, with powerful image capture and processing capabilities. Cameras and ambient light sensors are also a good choice if difficulties in actively synthesizing images for transmission to the camera, and the line-of-sight requirement can be solved.
- Magnetometers or Digital compasses are another class of sensors that have gained popularity in mobile phones. The heart of this solution is tri-axial vector magnetometer sensors, which are able to sense the magnitude of the surrounding magnetic field along their sensitive axes.

Sensors in mobile devices have been introduced mainly to enhance user experience. After the initiative of application programmable interfaces to these sensors, it has become common to use, usually in combination with each other, for context recognition [17]. Some of the most commonly used sensors in context recognition include accelerometers, proximity sensors, light sensors, Global Positioning System (GPS), compasses, gyroscopes, microphones, cameras, and Bluetooth. Using entire data from sensors for high quality context recognition can be as tempting as possible. However, this comes with a cost of higher power consumption. The more sensors the application uses, the shorter the battery lasts [18].

User authentication methods

To make life easier for smartphone users and to increase the joy of using communication devices, a solution might be to implement different security levels for accessing different types of data or applications. The combination of novel authentication methods, such as biometric authentication or memory-based authentication means a gradual approach to security which may increase the overall protection. Based on individual preferences, the usage of smartphone can be safer while maintaining a manageable level of complexity. There is another dimension which has to be pondered: the simplicity and acceptance of the respective method. When thinking about a suitable authentication method, a very complex and intrusive choice may be adequate for a very sensitive and rarely used application, but users will not choose it for an even more sensitive application which they have to use very often.

The user authentication method indicates the entire process where a user, who requests his approach to the system, is authenticated as the user himself by verifying his authority or qualification with which he can reach data in the system. The entire authentication process is composed of 1) identification that a user claims as his qualification, 2) authentication through an authentication server to prove that user who requests access is allowed, and 3) an access control mechanism-based authorization where the server allows the user to use the system resources [6,19]. In particular, the authentication process is an essential requirement in permitting a user to receive services given by the service provider. Three major types of authentication means are demonstrated in **Table 1** [12].

Table 1 Authentication means, classified by types.

Classification	Description	Type	Example
Type I	Something you know	Knowledge-based	Password, PIN
Type II	Something you have	Token-based	Smart card, Token
Type III	Something you are	Biometric	Iris, Fingerprint
	Something you do	Biometric-context	Voice, Signature

Classic authentication factors mostly used can be categorized into 3 groups [13]:

1) Knowledge-based or "something you know"

Knowledge-based authentication factors rely on a memorized piece of information, e.g. a PIN or password. Long and random password can offer a high level of security in authentication systems. However, in practice, user has huge difficulties in memorizing random and strong passwords. This is often resulted in the use of short password that is therefore simple to guess and does not provide high authentication security.

2) Object-based or Token-based or "something you have"

Object-based authentication factors rely on physical possessions, e.g. tokens. A token has the advantage over a knowledge-based authentication factor such that user does not need to memorize anything.

3) Identity-based or "something you are" and "something you do"

Identity-based authentication factors cover both basic biometric and biometric-context methods which rely on the uniqueness of the physiological (e.g. fingerprint, facial features) or behavioral (e.g. hand-writing, speech) characteristics of the owner. Biometric-based authentication offers two advantages over the other classic authentication factors:

- The owner does not need to remember or carry anything.
- The verification of the genuine owner is processed at the location of the biometric sensor.

However, biometric authentication systems are not perfect, and their security can also be undermined.

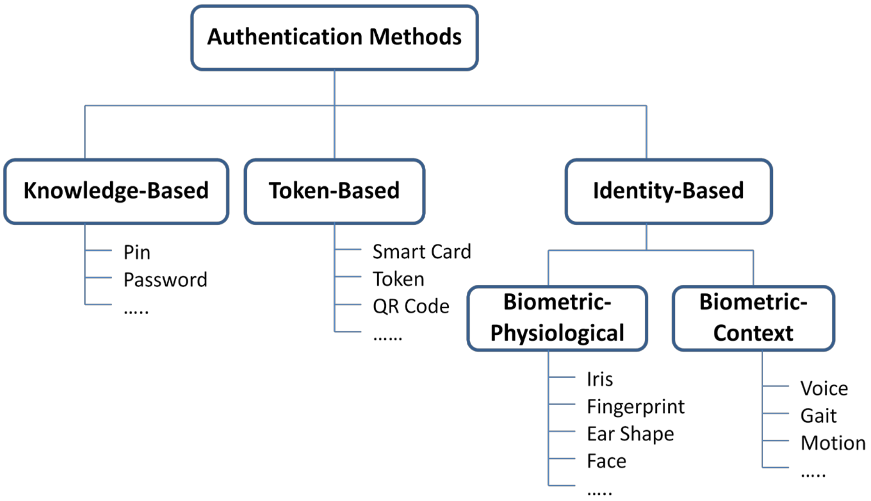

Figure 1 Classification of authentication methods.

Comparison and discussion of different approaches based on authentication mechanisms

Several surveys deal with the security needs of mobile phone users. Experimental results towards various authentication methods had been reviewed to illustrate the advantages and disadvantages of different approaches. The existing authentication methods can be divided into 3 groups as illustrated in **Figure 1**.

Knowledge-based authentication

Knowledge-based authentication via a PIN or password is the most common method, and has long been embedded in almost every mobile device. Generally, in the context of mobile devices, a PIN is often used for authentication with the Subscriber Identity Module (SIM)-card after starting the phone, while a password is used to protect the smartphone from unauthorized access and use.

Table 2 Novel techniques of knowledge-based authentication.

No.	Ref.	Knowledge	Key	Technique	Approach	Pros/Cons
1	[20] 2005	Graphical password	Password	PassPoints: Design and longitudinal evaluation of a graphical password system	The image defined could be provided by the system or chosen by user. A user password consists of any arbitrarily chosen sequence of points in the image. Practically, the image must be intricate and rich enough. There are no prior artificial predefined click regions with well-marked boundaries. In order to log in, the user has to click close to the chosen click point, within some set of tolerance distance.	Pros: Large password spaces then textual password. Cons: More difficult to learn the password than a textual password.
2	[21] 2011	Graphical password	Password	Matrix values of Image	The authentication process is granted by selecting an image of a matrix value corresponding to the query that is synchronized in advance between the service server and the smartphone. The service server requests the user to input an existing flexible combination of text-based and graphic-based password for authentication.	Pros: Uses a combination of sensors which provides more accuracy. Cons: Multi-level authenticating, include-ing system training and comparison with a pre-defined database. Intensive time and power consumption.
3	[22] 2011	Graphical password	Password	A mixture of both recognition and recall based schemes	During registration, the user selects a user name and a textual password and then chooses an object as password by drawing. The object will be stored in the database with his username. During authentication, the user first gives his username and textual password and then draws pre-selected objects.	Pros: More secure according to the use of a combination of textual and graphical password. Cons: User without drawing capability can arouse log-in error.
4	[23] 2011	Use physical proximity to guarantee security	PIN	A modulated illumination of mobile device screens to transmit PIN	User enters a PIN on his mobile device in a PIN-entry-window. The PIN is transmitted via temporally varying patterns of light shown on the device screen. The light patterns are sensed using commodity electronic components integrated	Pros: Assures confidentiality against MITM attacks. Cons: Light sensor works within limited geographic scope.

No.	Ref.	Knowledge	Key	Technique	Approach	Pros/Cons
					into the receiver unit.	
5	[24] 2012	Location APIs	Location	Location-based authentication and authorization using smartphone	Two types of location information are used: static (registered) and dynamic (captured every time the user requests access) location. The crucial part is location verification, which utilizes LAT, LNG coordinates obtained from two different location APIs. The location claimed is verified for its validity, compared to specified authorized location, and a decision is made whether the user is authenticated or not. The security of the whole system can either succeed or fail depending on the effectiveness of the location-verification.	Pros: Uses built-in function within the mobile. Cons: Overlap in location can induce errors in verification.
6	[25] 2013	Graphical password (Drawmetric System)	Password	The marbles authentication approach	A password comprises an arbitrary sequence of marbles (colors). After a marble is dragged in the center, it immediately reappears on its prior position. The position is kept during one authentication but rearranged at the beginning of each new attempt. One repeated color is allowed. To authenticate, the user is required to drag the digits in the right order into the center of the screen. The position of the marble arrangement is also kept as one of the authentication criteria.	Pros: Password space has no upper restriction in this approach Cons: User is required to recognize the pattern of key arrangement.

Secret drawing [20- 22,25] seemed to be more entertaining method for users, although it may take some time for users to memorize the patterns. Some of these techniques have illustrated adverse results; for example, graphic-based authentication results [25] have shown an error rate of 9.5 % (192 test-sessions) based on all authentications. The hybrid graphical password system, a mixture of both recognition and recall based schemes [22], have shown surprising records of provable resistance to many varieties of attacks, such as Brute Force, Guessing, Shoulder Surfing, Phishing, Dictionary and Spyware or Naïve Key Logging. Nevertheless, when it comes to selecting graphical password, users tend to choose symmetrical figures, making the password space small, and again, easy to break [21,22]. A scenario where an adversary steals the secret by spying (e.g. with a camera) on a user while they input the secret (password or drawing) is given as an example in [26], which shows the vulnerability of the "smudge attack" to the Android password pattern. A snapshot of the smartphone screen taken can allow attacker to reconstruct the pattern drawn by a user on the touch screen to unlock the phone. The light reflex of the smudge left on the smartphone can also be leveraged by attackers. The solution to Smudge Attacks is a recognition-based password involving the drawing of a pattern [20,25]. Thus, the concept of access is granted only if a pattern of keywords matching the stored record is presented [24]. Notwithstanding this, the pattern of finger movement or the exact shape of the drawing seems to be a difficult task for users.

Location cross-checking is a popular technique that has been integrated into authentication systems as a factor to counter distance attacks, since it does not require additional receivers to be installed for location verification. Instead, location cross-checking compares the actual location of the smartphone with a pre-agreed set of known points of businesses related to the registered clients. However, the ongoing monitoring of location-tracking is difficult to maintain, as smartphone might be switched off, or might be used outside the traceable area. A further downside on the restriction of those sensors is that GPS cannot be used indoors, or in urban areas, with many high glass-front buildings, where a direct line of sight to the satellites is not available. Wi-Fi-based positioning seemed to be a better choice, since it works indoors effectively, as well as outdoors, as long as the AP transmitted beacon can reach the smartphone. However, the number of available APs differs greatly between urban and rural areas, making Wi-Fi-based positioning a technique used mainly in big cities with lots of existing and known APs [13].

PIN has usually been the only security mechanism used in mobile phones for decades. It is normally used to identify the user in the network when the device is turned on, but it can also be used to lock the keypads. The use of PIN and modulated patterns of light shown on the screen, sensed by a cheap bespoke receiver unit, is seemed to be a better choice [23]. The test results of an experiment in a dark room, indoors, and open spaces have shown a passable error in communication at an average of 3.6 %, while the observable attack results where attacker successfully retrieves an entire PIN is 0 %.

Drawbacks occur when the authorized user selects simple or guessable combinations, share or use the same codes for multiple purposes and accounts, or even write the secret codes down [18]. Usability and security issues often urged from the scenario where user inputs his code in public settings; the input can then easily be observed by an attacker, and the user's password or PIN is exposed. Furthermore, user tends to activate his device and keeps it active for long period of time. The longer he lets his mobile phone stay active, the more insecure the mobile phone is. Besides, this method also asks for awareness from the user, which often leads to annoyance. Hence, the area of PINs/passwords authentication has long been an unpopular field for exploration [5].

Object-based authentication

Token or object based authentication methods are used on a regular basis by many people around the world. There exist various approaches of hardware and software tokens. Hardware-based may range from contactless proximity cards to regular contact smartcards inside the mobile phone itself, whereas software-based may present in the forms of One Time Password, QR Code, etc. The authentication software may have some advantages over hardware, through a fast and easy completion of the authentication procedure.

Table 3 Novel techniques of object-based authentication.

No.	Ref.	Token	Object	Technique	Approach	Pros/Cons
1	[27] 2010	Dynamic Keystroke Pattern	Mobile time Registration token	Trustable Keystroke-Based Authentication for Web-Based Application	While the user enters his password, the keystroke monitor records the keystroke dynamics. Keystroke pattern is sent to a Trusted Third Party (TTP), which then performs attestation of the mobile device to establish trust in the reporting entity. Once trust in the keystroke monitor and the keystroke pattern is established, the TTP will match the pattern and grant authentication. Then TTP will return a token to the mobile browser.	Pros: Gets rid of issues of accessibility of user's keystroke entry pattern on browser-based applications. Cons: Requires extra steps, such as user having to register each type of keyboard with the TTP in advance.
2	[7] 2011	Magnetic Token and Acoustic Token	1. Compass 2. Acoustic transmitter	1.Static magnetic fields 2.Sound waves	1. Magnetic Token: The token emits electromagnetic waves by virtue of varying the magnetic field around the inductor. For access to remote	Pros: Less prone to snooping. Cons: A sharp drop in the strength of the

No.	Ref.	Token	Object	Technique	Approach	Pros/Cons
					services, a PIN can be transmitted on demand. The orientation of permanent magnets in the encoding is similar to credit card magnetic strips. 2. Acoustic Token: offers higher communication bandwidth at lower power consumption compared to digital compass. On the receiver device of the smartphone, the carrier frequency is isolated, then decoded.	magnetic field created can cause difficulties to user.
3	[28] 2012	Smartphone as a unique hardware token + a password or others tokens established by the IDP	Smartphone	2-factor authentication using smartphone for logical and physical resource access in a single sign-on environment.	To perform physical access, session data is transferred from the smartphone to the authentication server through QR codes. To authenticate the user to access the service, a smartphone with a working SIM card is required to connect to the internet. The Identity Provider will use an LDAP server to store the IMEI and IMSI of user which are unique identifiers associated with the mobile phone and SIM card.	Pros: High security; attacker is required to assume both mobile and IMEI for impersonation.
4	[17] 2012	Personal Identity Number (PIN) + Init-Secret+ Epoch Time	Time Synchronous	Software Token Based Two Factor Authentication Scheme	Authentication is based on two factors: a PIN known by the user and the Init-Secret stored on the mobile device. A one Time Password (OTP) valid for 60 seconds is generated after the user enters his PIN. To compensate time differences, the server will accept passwords from 3 min in the past to 3 min in the future. The time must be synchronized with the client and the server to ensure the correct password is generated each time.	Pros: The hacker has to know both the PIN and Init-Secret in order to steal and crack the password. Cons: Low protection if the mobile is lost. The attacker can retrieve the PIN from shoulder-surfing attack.
5	[29] 2012	Smart card + PIN	NFC-enabled mobile phone as a chip card reader for contactless smart cards	Mobile smart card reader using NFC-enabled smart-phones	Using an NFC-enabled mobile phone as a chip card reader, a mobile phone can be used to visualize, inspect and control electronic transactions. The PIN is managed as a temporary PIN if the card is used on a terminal that does not support external readers. When all transactions with the terminal are completed, the smartphone changes the PIN back to a permanent secret PIN.	Pros: The concept of a temporary pin has reduced the possibility of attacker to track a permanent pin. Cons: A computer or public terminal is required as an input and output device for the smart card.
6	[30] 2012	QR Code	Personal Token	User Authentication System Using QR code Identifying	When a user requests the service provider to allow his access to the service, the service provider will extract the client's information,	Pros: Low cost, ease of use and reduction in need for human memorization.

No.	Ref.	Token	Object	Technique	Approach	Pros/Cons
				Method	generate a QR code and transmit it to the client. When the QR code is presented on the client screen, the user scans the QR code with his registered device and can request the service provider to authenticate.	
7	[31] 2013	Touch-screen based Authentication	Light Sensor	FUEL: Fast, ubiquitous, easy-to-use, and low-cost authentication for smartphones	When a user wants to log in, instead of entering a password, he just has to place a hardware token that emits light on the surface of the smartphone in accordance with a key bit string encoded for security. The secret bit sequence is relayed through the LED, and verified by the smartphone; authentication is then granted.	Pros: Low cost and high efficiency. Cons: Error can occur from the line-of-sight constraint and the guard around the token light emitter.

Table 4 Varieties of hardware and software tokens adopted for object-based authentication.

Tokens	Hardware	Software	1[28]	2[7]	3[28]	4[17]	5[29]	6[30]	7[31]
Time Registration		✓	✓						
Magnetic/Acoustic Signal	✓	✓		✓					
Smartphone/Sensors	✓	✓			✓				✓
Personal Identity (e.g.: QR Code)		✓				✓		✓	
Smart Card (NFC)	✓	✓					✓		

Token-based hardware

Hardware tokens are any devices or objects that can authenticate a user. They are available in various forms, such as a smartphone's compass, a mobile handset [7], or an easy-access device, such as key fobs, watches, smartphones, or built-in sensors [28,29,31]. Common modern examples include physical keys, proximity cards, credit cards, or ATM cards. In the case that higher security is requested, a 2 factor authentication can be naturalized to help lower the number of cases of identity theft on the Internet, as well as phishing via email because the criminal would need more than just the user name and password details. Varieties of advertent 2-FAs have been introduced, such as PIN and OTP [17] or PIN and smartcard [29]. Tokens are good because they are simple. Physical keys, for example, are widely supported, cheap to produce and use. However, tokens have their own weaknesses, because although tokens are simple and cheap to produce, they are also simple and cheap to reproduce. This makes them vulnerable to counterfeiting. Also, because they are typically a physical object or device, they can be stolen more easily than passwords. The obvious problem is this technique demands user to carry something with him to be presented for an authentication; many users would likely find it unwieldy, and would presumably leave the token attached with the device for convenience.

Token-based software

Some software tokens may require extra setting [27] while some may not [17,28]. For example, keystroke-based authentication requires user to register each type of keyboard pattern with the TTP beforehand [27]. Keystroke-based authentication is an effective approach, but the predefined part has annoyed user. Therefore, instead of detecting the user identity by asking him to identify himself by inputting through a virtual keyboard, a QR code has become an effective replacement. Most mobile phones are equipped with cameras and can activate QR code reader software [28,46]; thus, during the actual authentication procedure, the information to authenticate and authorize the QR code can be transmitted to a preselected identity provider. QR code authentication is rather difficult for attacker to steal information or to guess the QR code, since it is not feasible for a person to recognize information stored in a QR code. Attacks such as Password guessing, Packet sniff, Man-in-the-Middle, Replay, Spoofing, Keyboard cracking and Web-cracking are effectively safeguarded against. The QR code is less efficient in comparison to the id/password system, which is less safe, but faster than the certificate system [30].

While knowledge-based authentication has already been indicated as inconvenient and not sufficiently secure, token-based authentication is proven to eliminate the risk of attacker guessing passwords easily from knowledge-based authentication. However, token-based authentication is inconvenient on account of demanding user to carry something with him. Since a token is needed to be present for an authentication, it is more likely to be always left attached to smartphone. The security drawback of physical tokens is that, when lost or stolen, an attacker gains unauthorized access to the devices. Then, the attacker can reprogram or change some security factors to serve their purpose. Theoretically, software tokens are less secured than hardware tokens because they can simply run on any electronic devices. Hence, the software-token can always be defeated by a hacker, who can divert a user's phone calls and SMS messages to a number controlled by intruders, so software tokens may be considered weaker still.

Identity-based authentication

Biometrics authentication seems to be the most promising techniques of authentication available nowadays, since it has seamlessly integrated the capabilities of sensors and mobile application together. The presence of the owner is considered adequate, without showing carry-on identities or remembering secret codes.

Table 5 Novel identity-based authentication.

No.	Ref.	Recognition	Sensors	Technique	Approach	Pros/Cons
1	[33] 2010	Iris	Camera	Daubechies Wavelet Transform	The processing consists of feature extraction and feature encoding. To extract the characteristic values of the iris, the image is quantized into 8 sub-images. For matching, a weight of each feature vector is assigned and a weighted similarity measure procedure is applied	Pros: High recognition accuracy rate. Cons: A few processes of feature processing are time and energy consuming.
2	[34] 2011	Image	Camera	Fragile watermarking based on Chaos Theory	The image is embedded with parameters of the chaotic function and the initial value of the chaotic watermark generation function. Changes to any of these factors will lead to a substantially different watermark signal. The comparable scheme then extracts the watermark pattern to legally authenticate. Extracting the right watermark is only possible if someone has correct keys.	Pros: Fast speed of authentication verification. Cons: Depends on a key which is not completely secured compared to other techniques.
3	[35] 2011	-User Motion -Voice	Accelerometer Microphone GPS, Wi-Fi,	-Sliding Window Based classifier aggregator	User motion- Signature of walking is collected for training and generating a binary classifier.	Pros: Uses a combination of sensors which should provide

No.	Ref.	Recognition	Sensors	Technique	Approach	Pros/Cons
		-Location History -Multi-Touch	Cell ID Touch Screen	- Naive Bayes binary classifiers	Location- uses location matching algorithm to compare the position of cell-id according to walking pattern. Multi-touch distance between the two fingers at the beginning and end is captured. The gesture specific features are extracted and forwarded to a detection engine to match against a user's profile.	more accuracy. Cons: Multi-level of authenticating, including system training and comparison with pre-defined database. Intensive time and power consumption.
4	[36] 2012	Arm Flex	Accelerometer + gyroscope	Cosine Similarity Euclidian Distance	Supports 2 types of operation: picking phone up from table and taking phone out from user's pocket. Every new signal detected by sensors will be evaluated against templates to produce a decision, as to whether one person is represented by a currently evaluated signal is an authorized person.	Pros: Fast algorithm. Cons: Threshold setup to identify users' behavior is sensitive to error detection rate.
5	[37] 2012	Behavior	Touch screen	Dynamic Time Warping (DTW)	Detects the way a user performs the password as a pattern. Uses common touch screen data in combination with the input of graphical passwords. The algorithm first compares 2 sets of time sequences then looks for similarities between the sets and calculates the cost to match one onto the other. The result is a warp distance that can be used to determine how similar a set is to the reference set.	Pros: Optimizing the threshold can improve the accuracy. Cons: Reference set must be defined for comparison. If the database is large, it can consume more time and energy.
6	[38] 2012	Image	Front-facing camera	Fast Semi-3D Face Vertical Pose Recovery	3-factor authentication feature; uses the 2 existing techniques: PIN code and serial number inside each mobile phone (IMSI). Added up with the evaluation of the vertical pose angle by the height difference between the center of eyes and the auriculo-cephalicsulcus of the pinna.	Pros: Extra security when combining with PIN. Cons: Using the camera causes quite high energy consumption which impacts the mobile battery.
7	[39] 2012	Gait	Accelerometer gyroscope	Feature selection-stepwise linear regression classifier-KNN	Uses physiological approaches to detect specific way that user holds the smartphone while using the applications loaded on the devices to discriminate the genuine user from the others. The intensity of the vibration caused by sliding the small touch panel of a smartphone is also detected. Accelerometer thresholds for detecting distinguished activities shall be afore-identified.	Pros: Similar efficiency to biometric based authentication. Cons: Relies on the ideal situation that the owner holds and operates the device in a similar style at all times.
8	[40] 2012	Gait	Accelerometer gyroscope	classifier-KNN	Gait and activity recognition are cooperatively applied to determine the relevant data where the subject is walking. The features extracted are then classified via a k-NN algorithm.	Pros: Does not require explicit user interaction during verification. Cons: Needs punctual calibration of accelerator and the recognition is

No.	Ref.	Recognition	Sensors	Technique	Approach	Pros/Cons
						only detected while walking.
9	[41] 2012	Finger photo	Camera	Edge-based approach image preprocessing	A photo of owner's fingers is taken automatically when an LED light is switched on. The most important criterion of the quality of a finger photo is the sharpness level. Then, the comparator will find the corresponding minutiae pairs in the reference and probe template. Later on, the training and test data is stored for distinguish reasoning.	Pros: Ease of use. Cons: Sensitive to camera limitations, such as noise, close distance focus, resolution, and light.
10	[42] 2012	Fingerprint	Camera	Rule mining	HuMan comprises 2 modules; a data collection module and a fingerprint generation module. The data collection module runs in the background to unobtrusively log information on calls, applications, browsing, etc. The fingerprint generation module resides above the data collection module to keep logs of Machine-recognizable rules and Human-memorable rules, as well as the user's fingerprints	Pros: Best fit in case of phone being lost. Cons: Poor performance.
11	[43] 2012	Finger Knuckle	Camera	Image preprocessing region segmentation feature extracted-1D log-Gabor filter	A contactless finger knuckle based personal authentication system. An acquisition of better quality images is necessary. Data will go through multiple image processes to detect finger knuckle features, matching them with the stored templates, and the result of authentication is presented to the (unknown) user.	Pros: Ease of Use. Cons: The execution time for the verification increases if the user stores many templates in the enrollment database. For accurate finger knuckle detection, a uniform background is required.
12	[44] 2012	Ear Shape	Camera	Image representation - Local Binary Pattern (LBP), Geometric Analysis Classifier KNN	The approach considers both shape and texture information in representing ear image. A composition of micro-patterns is described by LBP. The concept that the user can adjust the location of the ear center is adopted to get geometric features. Then, the combination of geometric features with LBP provides a representation of ear. For classification, the nearest neighbor classifier is used.	Pros: High recognition rate Cons: More impact from external factors.

Table 6 Novel concepts on physical/behavioral based biometric authentication.

Biometric authentication	**1[33]**	**2[34]**	**3[35]**	**4[36]**	**5[37]**	**6[38]**	**7[39]**	**8[40]**	**9[41]**	**10[42]**	**11[43]**	**12[44]**
Gait Recognition			✓	✓			✓	✓				
Voice Recognition			✓									
Screen Touching pattern			✓		✓							
Face Recognition		✓				✓						
Finger/Fingerprint/Finger Pattern			✓						✓	✓	✓	
Ear Shape												✓
Iris Scan	✓											✓

Table 7 Summary of sensors applied in identity-based authentication.

Biometric authentication	**1[33]**	**2[34]**	**3[35]**	**4[36]**	**5[37]**	**6[38]**	**7[39]**	**8[40]**	**9[41]**	**10[42]**	**11[43]**	**12[44]**
Accelerometer			✓	✓			✓	✓				
Gyroscope			✓	✓			✓	✓				
Microphone			✓									
Camera	✓	✓	✓			✓			✓	✓	✓	✓
GPS			✓									
Touch Screen			✓		✓							

Identity-based or physiological biometrics identifies the user based on his physiological features. Examples include: face recognition [34,38], user motion recognition / gait recognition [35,36,39,40], voice recognition [35], finger recognition [41,43] (i.e. memorizing the fingerprint, finger knuckle, finger line), ear shape recognition [44], iris scan [33], or a combination of those attributes, as described in **Table 5**.

There is a proven evidence that some good recognition rates can be obtained when using the geometric recognition of **External Ear Shape**, when a user holds the mobile phone at the position of his ear [44] (a recognition rate of 92.5 %). Nevertheless, this method is heavily influenced by external factors; it is hard to transparently get a useful picture of the ear, or get useful acoustic feedback that characterizes the exact shape [14]. For example, the ear might be obstructed by hair or because the user is wearing a hat or veil. Besides, the camera must be used at an appropriate position to get the correct focus on the target with enough illumination.

Face Recognition [34,38], one of the most popular features in the biometric technique range, has shown to provide an impressive recognition rate. For instance, the concept of face image authentication through a watermark generated by a pseudo-random chaotic process [34], as well as the technique of Fast Semi-3D Face Horizontal Pose Recovery [38]. The latter shows 91 % accuracy which is higher than the other techniques. Moreover, the combinations of face recognition and other biometric signatures, such as a teeth shape scan, palm shape, or finger line, have been suggested to be set up as an on-board database so that user may have choices when they want to use any of them for authentication [3]. At any rate, the algorithms appear to be sensitive to variations in illumination, such as the illumination changed may result in a significant performance drop; the changes in the angle of the face position also has an effect on performance, e.g. at an angle of more than 30 degrees difference, recognition becomes ineffective [8].

Despite the inherent technological challenges, **Voice Recognition** [35] has attracted abundant users, because they can use a microphone which is easy to access for user identification likewise the basic concept of Google Glass. However, there are several limitations which can make the recognition suffer, such as different people are possibly to have similar voices, and anybody's voice can vary over time because of changes in health, emotional state, and age. In addition, background noise, or the properties of the smartphone, such as low battery or low transmission of the signal, can greatly complicate recognition.

Obviously, voice by itself does not currently provide sufficient accuracy, it should be combined with another biometric, like face or fingerprint recognition.

Fingerprint and finger modal [35,41-43] biometric technology is commonly used to replace password-based security. Fingerprint swipe sensors have been incorporated for secure access in some models of smart devices. Instead of typing a username, the user can just place finger on a scanner in his mobile device. The system then verifies his identity. Based on a survey on the needs for different security methods on mobile phones [18], fingerprints are the most accepted and adopted method among users (74 %). Varieties of finger modality are applied as an authentication tool; for example: finger knuckle, finger line, and finger shape. Yet, there are some variables associated with the system's failure in the process of acquiring images of adequate quality, such as scratches on finger prints, the swelling of fingers, and the quality of light, which can cause problems similar to face recognition. These failures result in high image quality error rates that can be directly correlated to false-reject rates. These techniques have been adopted as biometric signature in numerous experiments due to the fact that they have long been used as a replacement for password, even on personal computers. However, the major obstacle to be considered is that the area that needs to be captured for fingerprint is small, and usually there is no occlusion that may intervene between the user's finger and the scanner [45]. In addition, this method also suffers by other highlighted problems, such as not being transparent to the user and most importantly, it cannot be leveraged by the technologies already available in smartphones.

Iris Scan [33] is another popular biometric technology which has been used to replace password input, similar to fingerprints. Among the present biometric traits, the iris is found to be the most reliable and accurate feature due to the rich texture of iris patterns, persistence of features through the life time of an individual and being neither duplicable nor imitable . However, during the process of scanning, if user blinks his eyes, have eyelashes or dust in the eyes, or even have bloat eyelid, the results may disturb the recognition. Of course, the illumination and the distance would also have impact on the quality of recognition.

The other classification of biometric measures is the **Behavioral Biometric or User-context**, where the user is identified based on his behavioral features, e.g. user motion [35], gait [39,40], screen touch pattern [37,39] and arm flex when replying to calls [36]. The arm flex context has achieved 87.8 % accuracy when picking the phone up from the table, and 90 % accuracy when picking the phone out of the pockets. Gait recognition are also seemed to earn advantages in the way that user can identify himself transparently to the device. In general, gait recognition is detected by the accelerometer and gyroscopic sensors, while the direction of movement is detected by the magnetometer [36,39,40]. Those remain problems in behavior detection, because the user is required to walk a certain distance from their mobile phone to be captured by its camera (mobile phones are usually carried in pant pockets, jacket pockets or handbags, making gait recognition by motion sensor unsuitable), or flex his arm in the same pattern in order to be identified.

In summary, these constraints result in a completely non-transparent authentication of the user. The physiological biometric is seemed to be more applicable technique at this moment. Within physiological biometric measures, methods that do not suffer much by obstruction problems are fingerprint recognition and ear recognition. Similarly, voice recognition remains the other good choice, but the requirement for extra devices, like a special device that is placed in the ear to emit acoustic signals and a special microphone that needed to be attached to the smartphone, still in thirst.

Performance issues of biometric-based

Biometrics is usually classified as physical or behavioral types. The physical type includes biometrics based on stable body features, such as fingerprints, the face, the iris, the ear and the hand palm. The behavioral type includes learned movements, such as handwritten signature, the mobile user's motion, and gait. Speech is usually categorized as behavioral because it is a product of learned behavior; however, the underlying body feature upon which speech is based is the vocal apparatus (lungs, vocal cords, nasal tract, vocal tract), which is physical and relatively stable. Yet, the key parameter for activity recognition is the position of the phone relative to the user's body. Thus, with the lack of user participation, such algorithms that require the execution of a calibration process that automatically identifies the device position prior to activity recognition will add a significant computational burden to the mobile phone, resulting in shortened battery life. Moreover, the classification methods, while being computationally simple, must be able to accurately recognize the user context and cope with the presence of unknown contexts, thereby providing scalability in the methods' context recognition techniques [8].

Physiological-based

In summary, the current physiological biometric solutions suffer from one or more of the following features:

(i) Non-transparent usage: illumination, positions and noise.

(ii) Performance: most of the recognizing patterns are normally time consuming due to the capacity of the database to store signatures. Hence, performance has become a major issue of this technique.

(iii) Lack of hardware on current smartphones: the limitation or hardware, such as microphones which are more likely built without noise detection, or cameras which always have problems with focusing, illumination, position or occlusion [8, 32], etc.

User-context based

Explicit factors affecting performance are:

(i) The effects of device position. The dependency of magnitude and the frequency of measured acceleration on the position of the accelerometer on the user's body has been highlighted [35,40].

(ii) The effects of device orientation. Not only the position, but also the orientation of the sensors has an impact on measurements of the magnetometer and the inertial sensors along their sensitive axes. In other words, considering the same user context and position of device, the values that are sensed on a sensitive axis of a sensor would not be repeated unless the same orientation is used. Consequently, a major challenge of mobile phone-based sensing systems is the effect of frequent change in orientation during everyday phone use and transport.

(iii) The efficiency of each of the processes within the user-context starting from feature selection, data classification and pattern recognition algorithms. Typically, it is preferable to use as few features as possible in mobile phone applications due to 2 reasons: first, the computational burden of feature extractions as the number of features increases, and second, the risk of obtaining suboptimal results due to classifier confusion, when too many features have been used. With optimum sensor data in the sensing stage, feature selection can confine the features to the most informative ones for a given sensor and the available classification technique.

Conclusions

Among the authentication methods available, knowledge-based and object-based authentication methods are used on a regular basis by a pluralism of people in real life. When biometric authentication methods are used to verify the person, they frequently involved in a transaction, create an inextricable link which can offer the property of non-repudiation. They are often seen as having advantages over other methods, because no secret key has to be remembered, no token or written-down note can be lost or stolen, and biometric methods are harder to "crack" [45]. However, implementing user-context processing capabilities without jeopardizing the user's overall mobile phone experience is a challenging task to prove.

The analysis has addressed the problems of the three main areas of authentication available such that user can select the best choice for the protection of his device. Highlighted merits and limitations, which user should be aware of, are as follows:

1) Knowledge-Based - A single password or PIN is an excellent authenticator. Its secrecy is a good defense against theft. It has a higher keyspace than most other authenticators; therefore it defends well against search attacks on the client. The remarkable advantages are its convenience and affordable price. The big debatable point encountered is memorization, which leads to controversies of graphical passwords. Graphical codes allow user to reproduce predefined drawings which can significantly improve his memory, especially when drawing the same shape repeatedly. This fashion of secret code is very close to biometric systems (e.g. handwriting recognition), but user often cannot redraw the scheme accurately enough, and he has a tendency to draw symmetrical images. Besides, the main barrier is not with maintaining a single password, but with multiple passwords. Humans have difficulty remembering these, so they choose easy-to-guess passwords, or they write them down and do not safeguard the content, which reduces efficacy. The password advantage has dried up because humans compromise security for the sake of convenience. The mechanism requires a smartphone to be available at all times. Moreover the authentication can take place in public areas, and thus is prone to shoulder surfing attacks. Even though the practice of single sign-on has reduced the password memorization burden, but is unlikely to eliminate it totally.

2) Token-Based - A token can provide a more substantial advantage when combined with a password. Tokens can store or generate multiple passwords, and this relieves user from having to remember multiple, changing passwords. A user is only required to remember only a single password to access the token: a single sign-on device. The other obvious advantage is that it provides detection because the absence of hardware token is perceptible. The 2 main disadvantages of tokens are the inconvenience and the cost. The equipment cost may be a little higher than a password. A combination of tokens and biometrics provides similar security characteristics to a token plus password. Intelligible hindrance is this combination is more likely to cost more from the cost of readers and it may be less convenient.

3) Biometric-Based - An apparent merit of biometric is that it is more difficult to be stolen than other authenticators. It provides a stronger defense against repudiation. In fact, all biometrics used for authentication depend on some degree upon physical body features; otherwise, there is no constant upon which to authenticate. These features are generated according to the model of the body when performing a certain action. Being driven from a body model, these features are more robust and less susceptible to the variability of performing different activities [46]. Various motion authenticators provide more reliable results than conventional signal-oriented features, without interrupting users from normal behavior. However, this approach is limited to situations where sensors have to be attached to some specific area of the body of a user. The heavy computational burden remains an issue for implementation on mobile devices. Differing from the discussed physiological-oriented features, user-context has recently started to attract the attention of researchers because it provides a more reliable alternative for physical activity recognition, unless the recognition rate for the dynamic signal, such as gait or voice; is high enough to provide security without inconveniencing the user with many false non-matches.

Therefore, the essential factors to be evaluated when selecting authentication schemes are expedience, charges, security, and risk assessment. If an authenticator is inconvenient, it will not be used, or will not be used properly, which may induce more vulnerabilities. User who must remember multiple, changing passwords is notorious for abusing password rules. Though a token reduces the problem of remembering passwords, the user must remember to carry the physical object, which is sometimes inconvenient. Although biometrics alleviates the problem of remembering, some users may experience inconvenience by false non-match results and short-battery life. Forasmuch as the tolerable cost of an authentication system is dependent upon the application, it is preferable to user to justify the cost resulting from an attack on his private information. The implementation of security to reduce the risk of successful attack must be chosen accordingly, depending on how user rate his data in terms of security levels. If information is less sensitive, weaker security mechanisms like passwords/PIN might provide sufficient security, following by the fact that weak security is always better than no security. Smart authentication systems in the future will indeed rely on multiple factors, or at least a combination of 2 authentication methods, to allow application specific access control decisions. In the near future, biometric systems tend to be an excellent addition to security and could be considered as substitution for token-based authentication, but they will never be a substitute for a username/password/PIN.

References

[1] V Kaushik. What's New in the World of Tapps, Techaheadblog, Available at: http://www.techaheadcorp.com/blog/technology/ten-countries-with-the-maximum-number-of-smart-phone-users, accessed September 2013.

[2] JM Watts. Thailand is Buying Record Numbers of Smartphones, but it's Facebook that People Really Want, Quartz, Available at: http://qz.com/98395/thailand-is-buying-record-numbers-of-smartphones-but-its-facebook-that-people-really-want/#, accessed September 2013.

[3] MF Islam and MN Islam. A biometrics-based secure architecture for mobile computing. *In*: Proceedings of the 2012 IEEE Long Island Systems, Applications and Technology Conference. Farmingdale, NY, 2012, p. 1-5.

[4] L Roalter, S Diewald, A Moller, T Stockinger, M Kranz and A Smith. Smartphone adoption and usage. Available at: http://pewinternet.org/Reports/2011/Smartphones.aspx, accessed September 2013.

[5] A Hang, F Hennecke, S Löhmann, M Maurer, H Palleis, S Rümelin, EV Zezschwitz, AButz and H Hussmann. *User Behavior, Technical Report*. University of Munich, 2012.

[6] T Dirflinger, A Voth, J Krimer and R Fromm. "My smartphone is a safe!", The user's point of view regarding novel authentication methods and gradual security levels on smartphones. *In*: Proceedings of the 2010 International Conference on Security and Cryptography, Athens, 2010, p. 1-10.

[7] H Bojinov and D Boneh. *Mobile Token-Based Authentication on a Budget*. Phoenix, Arizona, 2011, p. 14-9.

[8] A Gluhak and R Tafazolli. A survey on smartphone-based systems for opportunistic user context recognition. *ACM Comput. Surv*. 2013; **45**, Article ID 27.

[9] DH Titterton and JL Weston. *Strapdown Inertial Navigation Technology*. 2nd ed. Institution of Electrical Engineers, New York, 2002.

[10] JS Yi, YS Choi, JA Jacko and A Sears. Context awareness via a single device-attached accelerometer during mobile computing. *In*: Proceedings of the 7th International Conference on Human Computer Interaction with Mobile Devices & Services. NY, USA, 2005, p. 303-6.

[11] Wikipedia, the free encyclopedia, Available at: http://en.wikipedia.org/wiki, accessed October 2013.

[12] PJ Phillips, A Martin, CL Wilson and M Przybocki. An introduction to evaluating biometric systems. *Computer* 2000; **33**, 56-63.

[13] T Kuseler and IA Lami. Using geographical location as an authentication factor to enhance mCommerce applications on smartphones. *Int. J. Comput. Sci. Secur.* 2012; **6**, 277-87.

[14] E Ferro and F Potorti. Bluetooth and wi-fi wireless protocols: A survey and a comparison. *IEEE Wirel. Comm.* 2005; **12**, 12-26.

[15] GPS Overview, Available at: http://www.csr.utexas.edu/texas_pwv/midterm/gabor/gps.html, accessed October 2013.

[16] E Kanjo, J Bacon, D Roberts and P Landshoff. MobSens: Making smart phones smarter. *IEEE Perv. Comput*. 2009; **8**, 50-7.

[17] M Singhal and S Tapaswi. Software tokens based two factor authentication scheme. *Int. J. Inform. Electron. Eng.* 2012; 2, 383-6.

[18] N Ben-Asher, H Sieger, A Ben-Oved, N Kirschnick and J Meyer, S Moller. On the need for different security methods on mobile phones. *In*: Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services. Stockholm, Sweden, 2011, p, 465-73.

[19] I Fischer, C Kuo, L Huang and M Frank. Short paper: Smartphones: Not smart enough? *In*: Proceedings of the 2nd ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. North Carolina, USA, 2012, p. 27-32.

[20] S Wiedenbeck, J Waters, J Birget, A Brodskiy and N Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Human Comput. Stud.* 2005; **1**, 102-27.

[21] H Hong-Kim, K Hun-Lee and Y Hoon-Jung. A design of authentication strengthening scheme using matrix values of image in smart phone environment. *In*: Proceedings of the 1st International Conference on Convergence and It's Application. Korea, 2013, p. 179-82.

[22] WZ Khan, MY Aalsalem and Y Xiang. A graphical password based system for small mobile devices. *Int. J. Comput. Sci. Iss.* 2011; **8**, 145-54.

[23] C Nickel. 2012, Accelerometer-based Biometric Gait Recognition for Authentication on Smartphones. Dissertation, vom Fachbereich Informatik der Technischen Universitiat Darmstadt, Germany.

[24] H Takamizawa and N Tanaka. Authentication system using location information on iPad or smartphone. *Int. J. Comput. Theor. Eng.* 2012; **4**, 153-7.

[25] EV Zezschwitz, A Koslow, AD Luca and H Hussmann. Making graphic-based authentication secure against smudge attacks. *In*: Proceedings of the 2013 International Conference on Intelligent User Interfaces. Santa Monica, CA, USA, 2013, p. 277-86.

[26] AJ Aviv, K Gibson, E Mossop, M Blaze and JM Smith. Smudge attacks on smartphone touch screens. *In*: Proceedings of the 4th USENIX Conference on Offensive Technologies. CA, USA, 2010, p. 1-10.

[27] M Nauman and T Ali. TOKEN: *Trustable Keystroke-Based Authentication for Web-Based Applications on Smartphones*. Springer-Verlag, Berlin-Heidelberg, 2010, p. 286-97.

[28] G Carullo, F Ferrucci and F Sarro. *Towards Improving Usability of Authentication Systems Using Smartphones for Logical and Physical Resource Access in a Single Sign-On Environment*. Springer-Verlag Berlin Heidelberg, 2012, p. 145-53.

[29] SD Ghogare, SP Jadhav, AR Chadha and HC Patil. Location based authentication: A new approach towards providing security. *Int. J. Sci. Res. Publ.* 2012; **2**, 1-5.

[30] A Bianchi, I Oakley and DS Kwon. Using mobile device screens for authentication. *In*: Proceedings of the 23rd Australian Computer-Human Interaction Conference. Canberra, Australia, 2011, p. 50-3.

[31] K Dhondge, H Park, BY Choi and S Song. FUEL: Fast, ubiquitous, easy-to-use, and low-cost authentication for smartphones. *In*: IEEE INFOCOM Student Session. Turin, Italy, 2013.

[32] YG Kim and MS Jun. A design of user authentication system using QR code identifying method. *In*: Proceedings of the 2011 6th International Conference on Computer Sciences and Convergence Information Technology. Seogwipo, 2011, p. 31-5.

[33] S Dey and D Samanta. Improved feature processing for Iris biometric authentication system. *Int. J. Electr. Electron. Eng.* 2008; **4**, 127-34.

[34] CP Hern and C Torres-Huitzil. A fragile watermarking scheme for image authentication in mobile devices. *In*: Proceedings of the 2011 8th International Conference on Electrical Engineering Computing Science and Automatic Control. Merida City, 2011, p. 1-6.

[35] W Shi, J Yang, Y Jiang, F Yang and Y Xiong. SenGuard: Passive user identification on smartphones using multiple sensors. *In*: Proceedings of the IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications. Wuhan, 2011, p. 141-8.

[36] AFP Negara, E Kodirov, MFA Abdullah, DJ Choi, GS Lee and S Sayeed. Arm's flex when responding call for implicit user authentication in smartphone. *Int. J. Secur. Its Appl.* 2012; 6, 879-83.

[37] AD Luca, A Hang, F Brudy, C Lindner and H Hussmann. Touch me once and I know it's you! Implicit authentication based on touch screen patterns. *In*: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Texas, USA, 2012, p. 987-96.

[38] JY Hu, CC Sueng, WH Liao and CC Ho. Android-based mobile payment service protected by 3-factor authentication and virtual private ad hoc networking. *In*: Proceedings of the Communications and Applications Conference Computing. Hong Kong, 2012, p. 111-6.

[39] CC Lin, D Liang, CC Chang and CH Yang. A new non-intrusive authentication method based on the orientation sensor for smartphone users, software security and reliability. *In*: Proceedings of the IEEE 6th International Conference on Digital Object Identifier. Gaithersburg, MD, 2012, p. 245-52.

[40] C Nickel, T Wirtl and C Busch. Authentication of smartphone users based on the way they walk using k-NN algorithm. *In*: Proceedings of the 8th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Piraeus, 2012, p. 16-20.

[41] C Stein, C Nickel and C Busch. Fingerphoto recognition with smartphone cameras. *In*: Proceedings of the International Conference of the Biometrics Special Interest Group. Darmstadt, 2012, p. 1-12.

[42] TK Wee, N Ramasubbu, D Lo, D Gao and RK Balan. HuMan: Creating memorable fingerprints of mobile users. *In*: Proceeding of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops. Lugano, 2012, p. 479-82.

[43] KY Cheng and A Kumar. Contactless finger knuckle identification using smartphones. *In*: Proceedings of the International Conference of the Biometrics Special Interest Group. Darmstadt, 2012, p. 1-6.

[44] A Fahmi PN, E Kodirov, DJ Choi, GS Lee, MF Azli and AS Sayeed, Implicit authentication based on ear shape biometrics using smartphone camera during a call. *In*: Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Seoul, Korea, 2012.

[45] P J Phillips, A Martin, C Wilson and M Przybocki. An introduction to evaluating biometric systems. *Computer* 2000, **33**, 56-63.

[46] A Zinnen, U Blanke and B Schiele. An analysis of sensor-oriented vs. model-based activity recognition. *In*: Proceeding of the International Symposium on Wearable Computers. Linz, 2009, 93-100.