Surveying the Development of Biometric User Authentication on Mobile Phones

Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou

***Abstract*—Designing reliable user authentication on mobile phones is becoming an increasingly important task to protect users' private information and data. Since biometric approaches can provide many advantages over the traditional authentication methods, they have become a significant topic for both academia and industry. The major goal of biometric user authentication is to authenticate legitimate users and identify impostors based on physiological and behavioral characteristics. In this paper, we survey the development of existing biometric authentication techniques on mobile phones, particularly on touch-enabled devices, with reference to 11 biometric approaches (five physiological and six behavioral). We present a taxonomy of existing efforts regarding biometric authentication on mobile phones and analyze their feasibility of deployment on touch-enabled mobile phones. In addition, we systematically characterize a generic biometric authentication system with eight potential attack points and survey practical attacks and potential countermeasures on mobile phones. Moreover, we propose a framework for establishing a reliable authentication mechanism through implementing a multimodal biometric user authentication in an appropriate way. Experimental results are presented to validate this framework using touch dynamics, and the results show that multimodal biometrics can be deployed on touch-enabled phones to significantly reduce the false rates of a single biometric system. Finally, we identify challenges and open problems in this area and suggest that touch dynamics will become a mainstream aspect in designing future user authentication on mobile phones.**

***Index Terms*—User authentication, mobile phones, multimodal biometrics, touch dynamics, behavioral biometrics, physiological biometrics.**

I. Introduction

SECURE and reliable user authentication has already become an important task in computing contexts [168]. With the popularity of mobile devices like mobile phones and their increasingly diverse capabilities like memory, users are likely to store much sensitive and private information (e.g., credit card numbers) on their mobile phones [106] and to use their phones for security sensitive tasks (e.g., authorizing commercial transactions) due to the fast speed of data connection and wireless connectivity [70]. Vendors were forecast to ship more than 1.8 billion mobile phones in 2013, while the number will be over 2.3 billion in 2017 [81]. This makes mobile phones become an attractive target for hackers and malware [47], [127], [191]. Therefore, it is very crucial and essential to develop a reliable user authentication mechanism on mobile phones for both academia and industry [19].

TABLE I
Existing User Authentication Methodologies

Method	Instances	Properties
What you know	ID, Password, PINs, etc.	Can be shared and forgotten
What you have	Cards, Keys, Badges, ect.	Can be shared and duplicated
What you are	Fingerprint, Face, Iris, etc.	Not possible to share and repudiate

User authentication methodologies can be broadly classified into three folders as shown in Table I. Currently, the most widely used techniques of user authentication are the passwords (or *passcodes*) and PINs (personal identification numbers), however, these techniques suffer from well-known limitations [168]. We particularly classify these limitations into two categories: *external factors* and *internal factors*. The former mainly refer to impostors and malware techniques. For example, passwords and PINs are easily acquired by direct covert observation, so once an impostor obtains the password, he/she can have total access to the user's resources [209]. By contrast, the latter mainly refer to users' habits like unsafe behaviors. For instance, users have difficulty in remembering complex and random passwords which is known as long-term memory (LTM) limitations [194], [220], thus, they may choose a very simple string, even the word "password" [26] and "123456" [201] as their secrets.

Regarding user authentication on mobile phones, the drawbacks of passwords and PINs still exist. Although authentication can also use tokens as alternatives, this kind of approaches does not lend itself particularly well in the above situation either [41]. To overcome the drawbacks of passwords and PINs based authentication, research is being done into biometrics-based methods for authenticating users on mobile phones, as biometric characteristics can be unique and not duplicable or transferable [142]. Generally, the main goal of applying biometrics to user authentication is to authenticate legitimate users and detect impostors in terms of users' physiological or

Manuscript received February 20, 2014; revised September 9, 2014 and December 20, 2014; accepted December 21, 2014. Date of publication December 31, 2014; date of current version August 20, 2015.

W. Meng is with the Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong, and also with the Infocomm Security Department, Institute for Infocomm Research, Singapore 138632 (e-mail: yuxin.meng@my.cityu.edu.hk).

D. S. Wong is with the Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong (e-mail: duncan@cityu.edu.hk).

S. Furnell is with the Centre for Security, Communications and Network Research, Plymouth University, Plymouth PL4 8AA, U.K. (e-mail: S.Furnell@plymouth.ac.uk).

J. Zhou is with the Infocomm Security Department, Institute for Infocomm Research, Singapore 138632 (e-mail: jyzhou@i2r.a-star.edu.sg).

Digital Object Identifier 10.1109/COMST.2014.2386915

behavioral characteristics. The concept of *biometrics* can be defined as below:

- An automated method of authentication by using measurable and enduring human physiological or behavioral characteristics to model and represent a user's identity.

In general, current biometric user authentication techniques can be categorized into two folders: *physiological* and *behavioral* approaches. The former usually use measurements from the human body such as fingerprint recognition [136], face recognition [217], iris recognition [186], retina recognition [121], and hand recognition [54]. On the other hand, the latter often use measurements from human actions such as voice recognition [206], signature recognition [140], gait patterns [138], and keystroke dynamics [20], [233]. With the rapid development of touchscreen mobile phones, touch dynamics [143] has gradually become a notable and popular topic for biometric authentication in recent years.

Motivation and Related Surveys: In literature, many surveys on biometric user authentication like [45], [68], [230] mainly focus on a very specific biometric area. For example, Duta [68] provided a survey associated with the technology used in hand shape-based biometric systems, Zhang and Gao [234] provided a survey of image-based face recognition, while Yampolskiy and Govindaraju [230] conducted a survey and classification regarding behavioral biometrics. In addition, these articles also did not target on mobile platforms.

For user authentication on mobile phones, an early survey was given by Clarke and Furnell [41] in 2005, whereas their work did not include touch dynamics, a relatively new input method with the recent advent of touchscreen mobile phones. Similarly, some other recent reviews/surveys like [97], [108], [135] and books like [13] described biometric authentication on mobile phones, while did not mention touch dynamics.

By contrast, some studies like [84], [173] recently introduced biometric authentication including touch behaviors on mobile phones, but these works did not give a comprehensive survey. On the whole, few surveys in literature provide a comprehensive overview regarding biometric user authentication specifically upon mobile phones. Therefore, in this survey, we aim to make up this gap by emphasizing the popularity of touch dynamics and investigating the development of biometric user authentication on mobile phones comprehensively.

To the best of our knowledge, this is the first comprehensive survey in the last *eight* years, which considers and emphasizes touch dynamics for biometric authentication on mobile phones. This also distinguishes our article from other related surveys. In addition, our work provides a comprehensive survey regarding the existing biometric authentication including both *physiological* and *behavioral* approaches on mobile phones, including touch-enabled phones. We hope that this effort could drive more research in this area.

Our Goals: The first goal of this article is to survey the development of existing biometric user authentication techniques on mobile phones according to *physiological* and *behavioral* approaches. We specifically introduce up to eleven biometric authentication techniques, present literature results by reviewing related articles and studies, and analyze their feasibility of deployment on touch-enabled mobile phones.

The second goal of this work is to systematically characterize the potential attack points for a general biometric authentication system, introduce practical attacks on (touchscreen) mobile phones and present potential countermeasures. We identify that a multimodal approach can provide a more reliable user authentication than a single biometric method.

The third goal is to characterize a framework for establishing a reliable authentication mechanism on mobile phones by appropriately implementing the multimodal biometric authentication mechanism, and to conduct a study to explain the application of this framework on touch dynamics-based authentication. What is more, we characterize and point out challenges and future trends in this area.

Contributions and Summary: To clarify the scope of this survey, we emphasize that we limit our discussions to the context of biometric approaches that are applicable for use on mobile phones.[1] As such, we do not consider or analyze wider biometric approaches such as mouse dynamics [4], or the use of biometrics in other application domains. Our contributions of this work can be summarized as below:

- Surveying the development of biometric authentication techniques including *physiological* and *behavioral* approaches on mobile phones and analyzing their feasibility of deployment on touch-enabled mobile phones.
- Characterizing a generic biometric authentication system, identifying eight potential attack points on mobile phones and pointing out promising countermeasures.
- Characterizing a framework for building a reliable user authentication mechanism, conducting a study and identifying challenges and future trends in this area. It is found that touch-enabled mobile phones will become a mainstream in mobile market and bring many new features (e.g., multi-touch) in designing future user authentication.

The remaining parts of this survey are organized as follows. Section II surveys the development of biometric user authentication according to *physiological* and *behavioral* techniques. Section III characterizes eight potential attack points for a general biometric authentication system and introduces potential countermeasures. Section IV characterizes a framework of establishing a reliable user authentication on mobile phones, presents a case study and summarizes six existing frameworks. Section V identifies challenges and future trends in this area. Finally, Section VI concludes this work.

II. Development of Biometric User Authentication

In this section, we divide biometric user authentication on mobile phones into two categories: *physiological* approaches and *behavioral* techniques, and describe their development by reviewing related articles and studies in an chronological order. Generally, physiological biometrics are related to the physical characteristics of a person such as fingerprint, face, iris/retina, and hand/palm, while behavioral biometrics have to do with the

[1] In this article, *mobile phone* mainly refers to a device that can make and receive phone calls over a radio link and we are not distinguishing between smartphones and the earlier types of cellular devices.

pattern of behavior of a person such as voice, signature, gait, keystroke dynamics and touch dynamics.

A. Physiological Biometric Authentication

Physiological biometrics are based upon a person's physical characteristics which are assumed to be relatively unchanging such as fingerprint, face, iris/retina, and hand/palm.

1) Fingerprint Recognition: This authentication technique may be the most widely known means of successfully identifying a person's identity and indeed were already being used in mobile phones. For example, Sagem MC959 handset in the year of 2000 incorporated a fingerprint recognition system into the back panel [183].

Fingerprint recognition is meanwhile a hot research topic on mobile authentication. Clarke *et al.* [39] surveyed around 160 users and identified that surveyed users responded positively towards the use of fingerprint scanning in mobile phones. Chen *et al.* [34] presented a prototype of secured mobile phones (particularly based on BIRD mobile phone) with embedded fingerprint recognition systems. They developed two modules: one is a front-end fingerprint capture sub-system and the other is a back-end fingerprint recognition system in smartphones. Then, Derawi *et al.* [65] proposed an approach of applying cell phone cameras to capturing fingerprint images and evaluated up to 1320 fingerprint images from some embedded capturing devices like Nokia N95. The results indicated that an equal error rate (EER) of 4.5% could be achieved. In addition, Sin *et al.* [199] proposed a template updating system for fingerprint verification where templates were replaced with matched inputs for a target structure. The system presented an ERR of 2% after updating in the evaluation and they further argued that their system was adopted on practical mobile phones in the commercial market from 2009. Afterwards, Liu and Song [134] proposed a real-time embedded finger-vein recognition system for authentication on mobile devices, with a finger-vein recognition algorithm. The experiments showed that the system could take only about 0.8 seconds to verify one input finger-vein sample and achieve an equal error rate (EER) of 0.07% on a database of 100 subjects.

There are also several evaluation and competition reports regarding fingerprint verification like the *International Fingerprint Verification Competition* (FVC) [82], which attempted to establish a common benchmark allowing both academia and industry to unambiguously compare the performance results based on their own fingerprint recognition algorithms [136]. The best ERR results achieved for the competition each year are 1.73% (2000), 0.19% (2002), 2.07% (2004), and 2.155% (2006), respectively.

Due to various reasons, some particular users are concerned about touching biometric scanners. To tackle this issue, touchless fingerprint authentication has been developed. For example, Ravi and Sivanath [170] proposed to use a camera to capture the user's finger at a distance. Then, the finger image obtained can be isolated from the background and fingerprint features can be extracted for authentication.

As fingerprint recognition can provide high authentication accuracy, more and more mobile firms recently started to integrate this technique with their developed new phones. In 2011, Motorola came up with fingerprint-based authentication with Atrix phones [100]. More recently, Apple applied the fingerprint recognition to the *iPhone 5s* in which the home button on this phone is also a fingerprint scanner [215], while HTC also released the newest Android phone of *HTC One Max* with a fingerprint scanner [46].

Fingerprint features: The features can be generally represented in two levels:

- Patterns: including arch, loop, and whorl.
- Minutia features: including ridge ending, bifurcation, and short ridge (or dot).

2) Face Recognition: The face (or facial) recognition system is an application for identifying or verifying a person from a digital image or a video frame using facial features, and it is a popular biometric technique which has received much attention from both academia and industry, due to the broad interdisciplinary nature of interest involved [165].

A lot of work has been done regarding face recognition on mobile phones. Abeni *et al.* [1] proposed a face recognition system based on one-class Support Vector Machines for mobile devices running the Symbian Operating System. In the evaluation, the recognition system was tested on a Nokia 6680 mobile phone and the results indicated that an EER of 7.92% and 3.95% could be achieved according to a global threshold and an individual threshold respectively. Then, Hadid *et al.* [87] proposed an approach of analyzing a face authentication scheme using Haar-like features with Ad-aBoost for face and eye detection. The obtained results were very promising and indicated the feasibility of face authentication on mobile phones. The achieved average authentication rates are 82% for small-sized faces (40 × 40 pixels) and 96% for faces of 80 × 80 pixels respectively. Tao and Veldhuis [208] developed a low-cost biometric authentication system for mobile devices from face detection, registration, illumination normalization, verification, to information fusion. Their system could be able to achieve an equal error rate of 2% in the experiment.

Later, Xi *et al.* [222] proposed a hierarchical correlation based face authentication (HCFA) scheme for mobile devices, which could analyze the relationship between each cross-correlation output peak generated from selected sub-regions of a face. They further implemented the scheme on Nokia S60 CLDC emulator using Java ME and the experimental results showed that the scheme suited resource-constrained mobile computing environment due to the low memory and storage demand. By testing on the Yale Face dataset B, their scheme could achieve an EER of 3.58%. Then, Findling and Mayrhofer [78] proposed a pan shot face unlock method: a mobile device unlock mechanism using all information available from a 180-degree pan shot of the device around the user's head. For face recognition, they evaluated different support vector machines and neural networks, and the results demonstrated the feasibility of their approach. Chen *et al.* [35] proposed a sensor-assisted facial authentication method, which used motion and light sensors to defend against 2D media attacks and virtual camera attacks. The experimental results showed that the approach could achieve 95–97% detection rate and 2–3% false alarm rate over 450 trials in real-settings.

For mobile firms, Apple has applied for a patent regarding a face recognition mechanism used to lock and unlock an iDevice system, in which the news was released by US Patent & Trademark Office in September 2012 [7]. The invention for a mobile device is to automatically lock systems based on determining that a user's face is no longer present in images captured by the device's built-in camera. At present, Apple has not finished implementing this technique on their products, but maybe in near future.

Face features: These features can be roughly classified into three folders:

- Traditional: relative position, size, and/or shape of the eyes, nose, cheekbones and jaw.
- Three dimensional: using 3D sensors to capture information about the shape of a face.
- Skin texture: using the visual details of the skin and turning the unique lines, patterns, and spots apparent in a person's skin into a mathematical space.

3) Iris Recognition: Iris is an elastic, pigmented and connective tissue that controls the pupil and it has a unique pattern from eye to eye and from person to person. In the mid 1980s, iris was identified as a good biometrics since no two irises are alike [96], [112]. Thus, the main goal of iris recognition is to identify a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance.

The use of iris as a means for personal identification may be started from some early works like [57], [58]. For instance, Daugman [58] provided the mathematical algorithms required for digitally encoding an image of an iris to allow comparison with a real time image.

Regarding authentication on mobile phones, Cho *et al.* [36] proposed a method of combining pupil and iris segmentation with eye images to improve the performance of iris recognition on mobile phones. Then, Park *et al.* [163] proposed a new iris recognition method on mobile phones based on corneal specular reflections (SRs), which can perform well in the case of user with glasses. The experimental results with 400 face images captured from 100 persons with a mobile phone camera showed that the rate of correct iris detection was 99.5% (for images without glasses) and 98.9% (for images with glasses or contact lenses) and that the consequent EER was 0.05% based on the detected iris images. Kang [104] later proposed a pre-processing method to improve the performance of iris recognition on mobile phones, due to limited computing power. There are three steps: automatic segmentation for pupil region; helper data extraction and pupil detection; and eyelids detection and feature matching. The experiment results showed that their approach could perform well and stably.

Iris features: The iris has many features that can be used to distinguish one iris from another, but one of the primary visible characteristics is the trabecular meshwork, which is an area of tissue in the eye located around the base of the cornea and gives the appearance of dividing the iris in a radial fashion [112].

4) Retina Recognition: This authentication technique uses the unique patterns on a person's retina for identification. The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye and each person's retina is unique.

It is worth noting that the retinal scan is often confused with the iris recognition mentioned above. They may be both categorized as 'eye biometrics', but their respective functions are completely different. The iris is located in the front of the eye, while the retina is located at the back. The retina consists of multiple layers of sensory tissue and millions of photoreceptors whose function is to transform light rays into electrical impulses. Thus, it is the blood vessel pattern in the retina that forms the foundation for retina recognition [55].

Retina scan requires the person to remove their glasses, place their eye close to the scanner, stare at a specific point, and remain still, and focus on a specified location for approximately 10 to 15 seconds until the scan is completed. Due to the high cost, this technique was primarily used in high security facilities (e.g., military installations) [55], but has not been officially implemented on mobile phones.[2]

5) Hand and Palm Recognition: In general, an individual's hand does not significantly change after a certain age, however, human hands aren't unique. In this case, the accuracy of hand recognition can be improved by combining with other individual features. In contrast, palm vein is unique to every individual, even among identical twins. Palms usually have a broad and complicated vascular pattern and thus contain a wealth of differentiating features for personal identification. Several survey articles regarding palmprint verification can be referred to [120] and [235].

Due to the size of hand and palm, they have not been widely adopted on mobile phones. But several research efforts have been made in literature. For instance, Han *et al.* [89] developed a sum-difference ordinal filter to extract discriminative features of palmprint using only '$+/-$' operations on image intensities for mobile devices. Then, Franzgrote *et al.* [74] proposed a hand orientation normalization method, which makes the palmprint acquisition on a mobile phone practical for use. They further conducted a performance study using an iPhone and demonstrated the feasibility of palmprint verification on phones. Moco *et al.* [149] proposed a real-time biometric recognition system based on palmprint images on a mobile device. This approach used orthogonal line ordinal features and the results showed that the best FRR of 8.52% and FAR of 0.01% could be achieved. Later, Aumi and Kratz [9] designed *AirAuth*, a biometric authentication technique that used in-air hand gestures to authenticate users tracked through a short-range depth sensor. This approach can track multiple distinct points on the user's hand simultaneously that act as a biometric for authentication. Choras and Kozik [37] later proposed a contactless palmprint biometrics by means of texture mask-based features for mobile devices.

[2] We noticed that some projects like [182] aim to deploy retina scan on mobile phone and there are several Android applications like Retinal Scanner for fun, but no formal application was released by mobile firms.

TABLE II
THE RESULTS OF PHYSIOLOGICAL BIOMETRIC AUTHENTICATION ON MOBILE PHONES WHICH CLAIMED BY RELATED WORKS

Method	**Works**	**Platform**	**Performance (%)**		
			FAR	FRR	EER
Fingerprint recognition	[34] in 2005	BIRD smart phone E868	-	-	4.16
	[65] in 2012	Nokia N95 and HTC Desire	-	-	4.66 (Nokia N95) 14.65 (HTC Desire)
	[199] in 2012	Simulated dataset	0.03	3.23	2.0
Iris recognition	[163] in 2008	Samsung SPH-S2300	-	-	0.05
Face recognition	[1] in 2006	Nokia 6680	-	-	3.95
	[87] in 2007	Nokia N90	4 (Average authentication error rate)		
	[222] in 2012	Nokia Series 60 (S60) emulator and Nokia N73	-	-	3.58 (expected)
	[35] in 2014	Samsung Galaxy Nexus	2-3 (Average false alarm rate)		

For mobile firms, some companies reported that they had implemented such technique on mobile phones such as Vodaphone in the UK [213] and Japanese Softbank Mobile Corp. in partnership with Universal Robot Co. Ltd. [231]. It seems that this kind of biometric authentication may become available on mobile phones in near future.

Discussions on physiological biometrics: Overall, an important and strong advantage of physiological biometrics is that the features come from the human body so that most of them are usually unique. The uniqueness of physiological biometrics makes them be able to construct a reliable authentication mechanism. For authenticating users on mobile phones (or touchscreen mobile phones), each of the physiological biometrics above has their own advantages and disadvantages. We analyze the feasibility of deploying these physiological biometrics on touch-enabled mobile phones as below.

- *Fingerprint recognition.* The fingerprint-based systems are often easy to use, cheap and require not much power. However, fingerprint patterns can be affected by cuts, dirt, or even wear and tear, and it is a complicated task to obtain high-quality images of distinctive fingerprint ridges and minutiae. This biometric technique has been implemented on touch-enabled phones (e.g., iPhones) and a special advantage is that users can use this biometric authentication during their touch gestures.
- *Face recognition.* The authentication can be done from a distance even without the user being aware of it, thus, it is non-intrusive, hand-free and generally accepted by users. But there are two main weaknesses: 1) it struggles to perform under certain conditions (e.g., angles); and 2) it may not work well under poor lighting, sunglasses, long hair, or other objects partially covering the face and with low resolution images. For authentication on touch-enabled phones, this biometric is easy to use and is very likely to be deployed by mobile firms based on [7].
- *Iris and retina recognition.* The benefits of using these biometrics are non-intrusive characteristic and high accuracy, but the main weaknesses of these biometrics are high cost and large time consumption (i.e., users must hold still while the scan is taking place). These biometrics are feasible on touch-enabled phones, whereas the high cost is a limiting factor.
- *Hand and palm recognition.* Generally, hand recognition is easy to use and non-intrusive, but it lacks of accuracy, fairly expensive and it needs a relatively larger scanner. In contrast, for palm recognition, it is non-intrusive and highly accurate, but the main weaknesses are high cost and inconsistent performance where the accuracy may be affected by body and ambient temperature. When authenticating users on touch-enabled phones, a reasonably large touchscreen provides a promising place to implement this kind of biometric authentication.

In Table II, we provide an overview of physiological biometric user authentication on mobile phones and available results from related articles regarding authentication accuracy. It is noticeable that the physiological biometrics-based systems, especially the iris recognition, can achieve a very high accuracy, showing the major advantage with respect to such kind of authentication approaches. However, they suffer from two major disadvantages when implementing on (touch-enabled) mobile phones:

- *Additional hardware.* Special and additional hardware is usually required to scan or recognize the physiological features which may greatly increase the implementation cost on mobile phones. Moreover, *liveness test* is a very important factor for such approaches which would further increase the cost, otherwise, biometric-print can be easily forged during user authentication.
- *One-off authentication.* Physiological biometric authentication is a kind of one-off authentication, in which the authentication is only performed at the beginning of a session and afterwards allows access for the duration of the session without re-authentication. This may leave a chance for impostors to access the current session and retrieve sensitive information from mobile phones.

B. Behavioral Biometric Authentication

Behavioral biometrics are based on a behavioral trait of an individual such as voice, signing a signature, gait, behavior profiling and typing rhythm (also called *keystroke dynamics*). With the advent of touchscreen mobile phones, *touch dynamics* has quickly become a hot topic for both academia and industry.

1) Voice Recognition: This biometric attempts to identify a person who is speaking by characterizing his/her voice. The key point is that each human has different voice signatures, and identical words may have different meanings if spoken with different inflections or in different contexts [18].

The idea of using voice as a biometric identifier has been proposed and developed for a long time. For authentication on mobile phones, Das *et al.* [56] proposed a speaker recognition method using a set of features called *Compressed Feature*

Dynamics (CFD), which could capture the speaker's identity from speech dynamics contained in the spoken passwords. They showed that this approach could achieve the best EER of 0.47% on a database with 79 speakers, where each speaker says 8 target passwords as well as the passwords from other 4 users. Miluzzo *et al.* [147] then presented *Darwin*, an enabling technology for mobile phone sensing that combines collaborative sensing and classification techniques to reason about human behavior and context on mobile phones. They further implemented a speaker recognition application to evaluate the benefits of *Darwin*. The experimental results showed that the application could improve the reliability and scalability without additional burden to users. Then, Kunz *et al.* [124] described an approach for continuous speaker verification during an ongoing phone call. Their developed prototype shows how it is possible to compute segments of a continuous audio signal in real-time. In the experiment, the approach achieved an EER of 15% with a segment length of 2 seconds. Later, Baloul *et al.* [16] proposed a speaker recognition approach based on a challenge-based method to defend against the replay attacks. Their experiments presented that an EER of 0.83% could be achieved on a PDA CMU dataset.

For mobile firms, Apple has developed an application called *Siri* in 2010 using the voice recognition technology, aiming to answer questions, make recommendations and perform actions by delegating requests to a set of Web services. Then, Lenovo IdeaPhone A586 [77] employed a speaker verification system designed by Baidu and A∗STAR's Institute for Infocomm Research to look for a specific voice signature, in which the phone can unlock without gestures or a longing stare when speaking a distinct passphrase. Later in May 2013, Barclays Wealth announced that a system was developed to verify the identity of telephone customers within 30 seconds of normal conversation by means of speaker recognition [218].

Voice features: The voice biometric authentication systems usually fall into two categories:

- Text-dependent: the text must be the same for enrollment and verification.
- Text-independent: no text constraints during enrollment and verification.

2) Signature Recognition: This technique measures and analyzes the physical activity of signing, while the core of a signature biometric system is behavioral. Traditionally, there are two ways to perform this recognition: *static* (i.e., signing on a paper) and *dynamic* (i.e., signing on a digitizing tablet). In the context of mobile phones, signature recognition is assumed to be dynamic, in which users should write their signatures in a digitizing tablet and in real-time.

In literature, Narayanaswamy *et al.* [155] studied the signature verification on mobile phones using a pen input. Then, Clarke and Mekala [43] introduced the application of signature biometrics to a mobile device in a transparent and continuous fashion. In the experiment, a total of 20 users participated in the study and an average FAR and FRR of 0 and 1.2 could be achieved respectively. Martinez *et al.* [140] conducted a study to investigate the effects of different mobile acquisition conditions for PDAs and smartphones. They proposed a signature verification system which combined Hidden Markov Models with score fusion. The experimental results indicated that their approach could achieve the best EER of 4% under random forgeries. Saevanee *et al.* [177] introduced a feasibility study of linguistic profiling, which could authenticate users based on their writing vocabulary and style of SMS messages. Then, Blanco *et al.* [15] conducted an evaluation in a mobile scenario using a database with 11 users and 8 mobile devices (based on stylus and finger). The experimental results presented that they could achieve the best EER of 0.17% and 0.29% using stylus and fingers respectively on Samsung Galaxy Note, while they could also obtain the worst EER of 3.48% on Asus. Then, Sae-Bae and Memon [180] proposed and studied online signature verification on touch interface-based mobile devices, which can be represented with a discriminative feature vector derived from attributes of several histograms that can be computed in linear time.

Later, 3D signatures (or called *magnetic signatures*) are proposed, which can be created on mobile phones using a properly shaped magnet (e.g., a rod or ring) taken in hand [103], [109], based on influencing the compass sensor embedded in mobile devices. Movement of the magnet in the form of a signature produces a temporal change in the magnetic field sensed by the embedded compass sensor, and can be used as a basis for authentication.

Signature related features: In order to recognize a signature, several features can be considered such as spatial coordinate of x at time t, spatial coordinate of y at time t, writing pressure, azimuth, inclination, pen up and pen down.

3) Gait Recognition: This type of recognition techniques is an emerging biometric technology which involves people being identified purely through the analysis of the way they walk. Currently, this kind of biometrics is still under development while it is feasible to be deployed on mobile phones as most phones like iPhones now can provide accelerometers with three primary axes (x, y, z).

Some research works have been made in literature. Mantyjarvi *et al.* [138] proposed an approach of identifying persons by using the acceleration signal characteristics produced by walking. The experimental results showed that the best EER of 7% was achieved by means of a signal correlation method. Later, Derawi *et al.* [64] provided a dataset with low-grade accelerometers, which was collected with a mobile device. Preproccesing, cycle detection and recognition-analysis were applied to the acceleration signal. The performance was evaluated with 51 volunteers and the results showed that they could achieve an EER of 20%. Frank *et al.* [80] proposed an approach for gait recognition based on a combination of feature extraction using time-delay embedding and supervised learning. They also designed an algorithm which was able to perform classification of activities in real-time on an HTC G1 phone. The results indicated that their approach achieved 100% test set accuracy on a noisy dataset consisting of 25 individuals. Nickel *et al.* [156] applied Hidden Markov Models for gait recognition and achieved a false non-match rate of 10.42% and a false match rate of 10.29%.

Then, Thang *et al.* [212] studied collecting gait data at the trouser pocket position and the data could be analyzed in both time domain and frequency domain. With a total of 11 volunteers in the experiment, they achieved an accuracy of 79.1% and 92.7% respectively. Meanwhile, Guerra-Casanova *et al.* [85] conducted a study of authenticating a person on a mobile device by gesture recognition. A user was prompted to be recognized by a gesture he/she performs moving his/her hand while holding a mobile device with an accelerometer embedded. By testing with a database of 100 users, equal error rates of 2.01% and 4.82% could be obtained in a zero-effort and under an active impostor attack respectively. Muaaz and Mayrhofer [152] then presented a gait recognition system by incorporating the Piecewise Linear Approximation (PLA) technique for mobile devices. The results showed that the approach could lead to design more robust and reliable gait authentication systems. Later, Choi *et al.* [38] proposed 6 gait signature metrics to represent gait characteristics of a user, which derived from the rate of changes of acceleration data. Their results showed that the proposed metrics were effective to identify individuals.

Gait related features: There are three main types of gait recognition:

- *Machine vision based*. The walk behavior would be captured by videos and video-processing techniques are used for analysis. For example, gait data can be captured by using various digital/analog cameras from certain distances. Later, different signal processing, image processing, and machine learning techniques are used for extracting gait-related information and identifying individuals [154].
- *Floor sensor based*. The sensors would be placed in the floor to measure force or pressure when an individual walks on them, and utilizing this information for identifying individuals.
- *Wearable sensor based*. The user wears a device aiming to measure the way of walking and recognize the patterns. This approach can use various types of sensors such as speed [62], accelerometer, gyroscope, and force sensors.

4) Behavior Profiling: This kind of techniques aims to identify people based upon the way in which they interact with the services of their mobile devices. During the authentication, current users' activities such as dialling a telephone number are compared with an existing profile (which is built from historical usage) through a machine learning method.

The research of behavior profiling was nearly started in late 1990s and can be divided into two categories: network-based and host-based approaches. The network-based approaches like [83], [88] are mainly focused on user calling and migration behavior over the service provider network, while the host-based approaches like [131] are based on the hypothesis that mobile users may use their applications differently in different time periods and at different locations. This article only considers and discusses the host-based approaches which can be performed on a mobile phone itself.

Regarding authentication on mobile phones, Li *et al.* [131] proposed a behavior-based profiling technique based on mobile user's application usage to detect abnormal mobile activities. The experiments on the MIT Reality dataset [71], [72] showed that an EER of of 5.4%, 2.2%, and 13.5% could be achieved for the telephony, text messaging and general application usage, respectively. Later, the same authors [132] described a feasibility study of behavior profiling technique using historical application usage to verify mobile users in a continuous manner and achieved an EER of 9.8%. Then they further proposed a novel behavior profiling framework in a modular way that would not reject user's access based upon not a single application activity but a number of consecutive abnormal application usages. The evaluation results on the MIT Reality dataset showed that this approach could achieve a FRR of 11.45% and a FAR of 4.17%, respectively. Then, Bassu *et al.* [14] proposed an approach to profile users' behavior with what, where, when, and how the devices were used. Meanwhile, Damopoulos *et al.* [50] developed an approach to profile the legitimate users on a mobile device like the iPhone based on touchlogger. For example, they showed that the touch events collected by the touchlogger could be utilized by an intrusion detection system (IDS) to detect misuses or intrusions. When compared to traditional keyloggers, they argued that a touchlogger could be at least equally hazardous to the user. In the evaluation, their approach achieved an accuracy of nearly 99% in a mode of post-authentication.

Behavior profiling related features: Taking the MIT Reality Mining dataset as an example, this dataset tracks and collects a large amount of people with their personal behavior and interpersonal interactions on mobile phones. There are two levels of application usage: *application-level information* (general applications) and *application-specific information* (voice call and text message).

- *General applications*: the information includes application name, date, time of usage and cell ID.
- *Voice call*: the information may contain date, time, number of calling, duration and cell ID.
- *Text message*: the information includes date, time, number of texting and cell ID.

5) Keystroke Dynamics: This dynamics utilizes the manner and the rhythm of an individual when typing characters on a keyboard or keypad. It was well-known and has been studied for a long time in authenticating users on mobile devices. For example, Clarke *et al.* [40] in 2003 first conducted a feasibility study of using keystroke dynamics to authenticate users on mobile handsets based on the way of typing. They indicated that a FRR of 9.8% and a FAR of 11% could be achieved using a neural network classifier. Then, Buchoux and Clarke [27] conducted a study and found that keystroke analysis could be implementable on a mobile handset technically and that users would be willing to adopt such an approach.

Afterwards, Rodrigues *et al.* [172] proposed a biometric authentication based on keystroke dynamics through numerical keyboards, which consists of five features (ASCII key code and four keystroke latencies). They argued that this approach could be applied to mobile phones. Then, Clarke and Furnell [42] extended the previous work [40] and conducted a study of authenticating users based upon their typing characteristics by entering telephone numbers and typing text messages. They found that neural network classifiers were able to perform classification with an average EER of 12.8%. Karatzouni and Clarke [107] then investigated the performance of keystroke analysis on thumb-based keyboards on smartphone devices. The results showed that this approach could achieve an average EER of 12.2% with the inter-keystroke latency based upon 50 participants. Campisi *et al.* [33] also conducted a study of keystroke-based authentication using a cellular phone keypad as input device. Their experiments on Nokia 6680 showed that the employed statistical classifier was able to perform user verification with an average EER of nearly 13%. Hwang *et al.* [95] proposed a scheme of keystroke dynamics by utilizing artificial rhythms and tempo cues. In the experiments with 25 users, they found that the proposed strategy could reduce the error to 4%. Then, Zahid *et al.* [233] showed that keystroke dynamics of a user can be translated into a viable features' set for accurate user identification. They further selected six distinguishing keystroke features such as key hold time, error rate, horizontal digraph, vertical digraph, non-adjacent horizontal digraph and non-adjacent vertical digraph, and developed a combined algorithm of PSO-GA-Fuzzy during the verification. The results showed that the best FAR of 2.07% and FRR of 1.73% could be achieved, respectively.

Then, Maxion and Killourhy [141] studied keystrokes by using only right-hand index finger in the restricted domain of numeric input and on an isolated keypad. In the experiments with 28 users, they achieved an unweighted correct-detection rate of 99.97% with a corresponding false-alarm rate of 1.51% by means of a random forest classifier. Later, Maiorana *et al.* [137] introduced a statistical classifier for performing user verification on mobile phones. Their approach relied on the analysis of keystroke dynamics referred to static text input. It is assumed that the timestamps generated by a mobile phone, and related to press and release events of a key can be acquired and processed. Their experiments on a Nokia 6680 mobile phone showed that the best EER of 13.59% could be achieved. Tasia *et al.* [210] proposed to combine two features like press pressure and press size in keystroke dynamics-based authentication on touchscreen devices. Giuffrida *et al.* [86] further proposed sensor-enhanced keystroke dynamics, in which the key idea is to characterize the typing behavior of users via unique sensor features and rely on standard machine learning techniques to perform user authentication. They argued that their approach could achieve the best EER of 0.08%. Kang and Cho [105] later showed that increasing the text length can further reduce the errors in authentication.

Keystroke dynamics related features: It is noted that different approaches could use various features like key hold time, latency, horizontal digraph, vertical digraph, error rate, etc.

6) Touch Dynamics: With the rapid development of mobile platforms, touchscreens have recently become a leading input method, which are an electronic visual display that users can control through simple or multi-touch gestures by touching the screen. It is expected that global touch screen shipments will reach 1.75 billion in 2013, among which approximately 1.28 billion or 73% are estimated to be for handsets, which will be a 14.2% on-year increase [229]. Thus, touch dynamics, which refers to collecting detailed information about individual touches such as touch duration and touch direction, has become very popular in mobile market and is an emerging hot topic in literature.

Regarding user authentication on mobile phones, Feng *et al.* [75] introduced a touchscreen-based approach and designed a finger gesture-based authentication system (called FAST) on touchscreen mobile devices. They selected a total of 53 features for each touch gesture and used a digital glove to capture 36 triaxial angular rate features when users performed touch activities. They conducted a study with 40 participants and the experimental results showed that FAST could achieve a FAR of 4.66% and a FRR of 0.13%, respectively. Then, Meng *et al.* [143] focused on touch dynamics and proposed a touch gestures-based biometric authentication scheme which consists of 21 features. They further considered *multi-touch*, which is the process of touching a touchscreen with multiple fingers at the same time, as one of the extracted features. The user study was conducted on Google/HTC Nexus One with 20 users and the results showed that the best FAR of 2.5% and FRR of 3.34% could be achieved using a combined classifier of PSO-RBFN. Later, Frank *et al.* [79] investigated whether a classifier could continuously authenticate users based on the way they interact with the touchscreen of smartphones. They selected 30 touch features that can be extracted from raw touchscreen logs and trained user profiles based on vertical and horizontal strokes using a k-nearest neighbor classifier and a Gaussian RBF kernel support vector machine. Their experimental results indicated that the classifier could achieve a median equal error rate of 0% for intra-session authentication, 2%–3% for inter-session authentication and below 4% when the authentication test was carried out one week after the enrollment phase. Sae-Bae *et al.* [181] also conducted a feasibility study and showed that multi-touch gestures are applicable for developing new user authentication techniques.

Later, Li *et al.* [130] designed a mechanism for smartphones to re-authenticate the current user's identity based on their fingers and touch movements. They particularly selected 8 sliding and tap related features and invited 75 users in their experiments, among which 25 were target and 47 were non-target users. During the verification, a support vector machine training model was created for each target user using positive examples (that belong to the same target user) and negative examples (that belong to the remaining target and non-target users). The results indicated that the best FAR of 4% and FRR of 4% could be approximatively achieved. Then, Meng *et al.* [144] developed a lightweight touch-dynamics-based authentication scheme with 8 features. They further developed an *adaptive mechanism* [145] to select an appropriate classifier in authenticating users with the purpose of maintaining the authentication accuracy. The experimental results showed that the scheme could achieve an average error rate of 2.46% (where FAR = 2.55%, FRR = 2.37%) by means of a PSO-RBFN classifier during the authentication. Afterwards, Xu *et al.* [227] also conducted a study and pointed out that touch operations such as keystroke, slide, pinch, and handwriting can be used to continuously authenticate users.

Comparison between touch dynamics and keystroke dynamics: Intuitively, touch dynamics is different from keystroke dynamics in that touch dynamics has more input types such as multi-touch and touch-movement, while keystroke dynamics only has key buttons as input devices, which does not have a

TABLE III
THE RESULTS OF BEHAVIORAL BIOMETRIC AUTHENTICATION ON MOBILE PHONES WHICH CLAIMED BY RELATED WORKS

Method	**Works**	**Platform**	**Performance (%)**		
			FAR	FRR	EER
Voice recognition	[56] in 2008	Database	-	-	0.47
	[124] in 2011	Simulated Dataset	-	-	15
	[16] in 2012	Simulated Dataset	-	-	0.83
Signature recognition	[140] in 2008	Simulated Dataset	-	-	4
	[15] in 2012	Samsung Galaxy Note	-	-	0.17 (Stylus) 0.29 (Finger)
Gait recognition	[138] in 2005	Portable device	-	-	7
	[64] in 2010	Google G1 phone	-	-	20
Behavior Profiling	[132] in 2013	MIT Dataset [71], [72]	4.17	11.45	-
	[50]in 2013	iPhone	< 1 (Average AER)		
Keystroke dynamics	[40] in 2003	Simulated Mobile Phone	11	9.8	-
	[172] in 2005	Pentium IV microcomputer	-	-	3.6
	[42] in 2007	Nokia 5110	-	-	12.8
	[33] in 2009	Nokia 6680	-	-	13
	[95] in 209	Samsung SCH-V740	-	-	4
	[233] in 2009	Symbian mobile phone	2.07	1.73	-
	[141] in 2010	Simulated Platform	-	-	1.45 (under constraints)
	[137] in 2011	Nokia 6680	-	-	13.59
	[86] in 2014	Samsung Nexus S	-	-	0.08
Touch dynamics	[75] in 2012	HTC Android smartphone	4.66	0.13	-
	[143] in 2012	Google/HTC Nexus One	2.5	3.34	-
	[79] in 2013	Android phones (e.g., Droid Incredible phones, Nexus One)	-	-	< 4 (related to scenarios)
	[130] in 2013	Motorola Droid smartphone	4	4	-
	[144] in 2014	Google/HTC Nexus One	2.55	2.37	-

movement feature. However, these dynamics also have some similarities. For instance, the inputs of press button-up and press button-down in keystroke dynamics are similar to the actions of touch press-up and touch press-down (e.g., single touch) in touch dynamics [143].

As touch dynamics has some similar actions to keystroke dynamics (e.g., touch press-down vs press down), some recent studies start to study touch typing behavior on touchscreens using a soft keyboard. For example, Cai *et al.* [32] exploited user interaction data of touchscreen mobile phone to authenticate users based on the way they perform touch operations. Feng *et al.* [76] studied the virtual key typing in authenticating mobile phone users. Later, Burgbacher and Hinrichs [28] proposed a classification framework on smartphones that could learn the gesture typing behavior of a person and decide whether a text message was written by the legitimate users.

In addition, some studies start to explore the effect of touch behavior on inputting passwords on touchscreen phones and present that combining touch dynamics with password input can enhance the authentication performance. Huang *et al.* [94] proposed a biometric authentication system through combining password and behavioral traits to authenticate user's identity on a mobile phone. Then, Oakley and Bianchi [157] explored the effect of multi-touch on inputting passwords and presented that the empirical data were broadly positive.

Touch dynamics related features: Different approaches can employ various touch related features on mobile phones such as single touch, multi-touch, touch movement, touch direction, touch pressure, touch size, etc.

Discussions on behavioral biometrics: As compared to physiological biometrics, behavioral biometrics may not be so accurate and stable due to the inconstancy of human behaviors. However, a strong and important advantage of the behavioral biometric authentication is that continuous and transparent authentication can be provided which can overcome the issue of one-off authentication. With respect to user authentication on mobile phones (especially on touchscreen mobile phones), each of the above behavioral biometrics has their own advantages and disadvantages.

- *Voice recognition*. The voice authentication is easy to use, widely accepted by users and allows remote authentication. In addition, the cost of implementation is relatively low and the storage size is small. But a major weakness is the high false non-match rates since the human voice may change under special conditions (i.e., when people get sick). This biometric technique has been implemented in current touch-enabled mobile phones like iPhones.
- *Signature recognition*. This biometric technique is highly resistant to impostors as it is extremely difficult to fully mimic the behavior of signing. Thus it is non-intrusive and is easily accepted by users. However, it is prone to high error rates because people may not always sign in a consistent manner. With the advent of touchscreens, this biometric is still feasible on touch-enabled phones when using a stylus, but cannot be used in a wide range.
- *Gait recognition*. This is a relatively new technique for authenticating users and the main advantage is that it can be applied for continuous verification of the identity of the user without his/her intervention. But many factors can affect its accuracy such as terrain, injury, footwear, fatigue, personal idiosyncrasies, etc. This biometric is feasible on touch-enabled phones whereas the authentication performance is a bottleneck.
- *Behavior profiling*. The main advantage of this biometric authentication is the capability of providing continuous

TABLE IV
SUMMARY OF ADVANTAGES AND DISADVANTAGES OF EACH BIOMETRIC TECHNIQUE

Biometrics	**Advantages**	**Disadvantages**
Fingerprint recognition	• Widely accepted and easy to use • The required power and cost is not high • Good accuracy	• Require additional hardware • High-quality image is not easy to obtain • Dose not work well under poor conditions such as cuts and dirt
Face recognition	• Widely accepted and easy to use • Non-intrusive and good accuracy	• Require additional hardware like camera • Does not work well under poor conditions such as poor lighting
Iris/retina recognition	• Non-intrusive • High accuracy	• Require additional hardware and high cost • Need more time for authentication
Hand recognition	• Easy to use • Less intrusive	• Require additional hardware like a large scanner • Medium accuracy affected by hand injury
Palm vein recognition	• High accuracy • Commonly accepted	• Require additional hardware like a large scanner • Expensive to implement
Voice recognition	• Widely accepted and easy to use • Remote authentication	• Relatively low accuracy • Does not work well under poor conditions such as illness
Signature recognition	• Widely accepted • Non-intrusive	• Relatively low accuracy • Require consistent writing trails
Gait recognition	• Continuous authentication • Can work without user intervention	• Low accuracy • The performance is easily affected by terrain, injury, etc.
Behavior profiling	• Continuous authentication	• Does not work well if users perform inconsistently
Keystroke dynamics	• Continuous authentication • Does not need additional hardware	• Does not work well if users perform inconsistently • Accuracy is inconsistent
Touch dynamics	• Continuous authentication • Does not need additional hardware	• Does not work well if users perform inconsistently • Accuracy is inconsistent

and transparent authentication when users interact with their mobile devices. However, a major weakness is the performance inconsistency when users interact with the mobile phones in an unusual way. This technique is feasible on touch-enabled phones when users are interacting with mobile applications.

- *Keystroke dynamics*. An important advantage of this dynamics is that no special hardware is needed. Moreover, it is non-intrusive and is able to capture the features without causing any additional overhead on users. But a major weakness is that it is hard for a keystroke dynamics-based authentication system to perform consistently if users perform unusually. With the advent of touch-enabled mobile phones, it seems that this dynamics will be gradually replaced by touch dynamics (i.e., current mobile phones provide less buttons), but it is still feasible on touchscreen mobile phones with soft keyboard.
- *Touch dynamics*. With the advent of touchscreens, this dynamics becomes popular for current mobile phones including Android phones and iPhones. The advantages and disadvantages are very similar to keystroke dynamics, but it provides much more actions that can be performed by users than keystroke dynamics such as touch movement, multi-touch, scroll, tap, flick, rotate, etc.

In Table III, we provide an overview of the existing behavioral biometric authentication techniques on mobile phones in the aspect of authentication accuracy claimed by related works. With the increasing capability of phones, it is noticeable that current phone-sensors are able to capture most users' behavior accurately, which make passive authentication become feasible and effective [195]. For example, Lane *et al.* [126] identified that current smartphones were effective at inferring complex human behavior through microphone, accelerometer and GPS information. Later, Zhu *et al.* [243] proposed a mobile system framework, called *SenSec*, which used passive sensory data such as accelerometer, gyroscope and magnetometer to ensure the security of applications and data on mobile devices. Their experiment validated that based on the collected sensory data, it is applicable and promising to validate users' motion and posture patterns when they are using the devices.

Due to the capability of sensors, touch dynamics gradually becomes a hot research topic in recent years. Overall, the main weakness of behavioral biometrics is that the authentication performance is not stable, while these biometrics have two major advantages as follows:

- No special and additional hardware is needed.
- Continuous and transparent user authentication can be provided.

Summary: As discussed above, we describe the characteristics of physiological and behavioral biometrics, respectively. In Table IV, we further detail and summarize the advantages and disadvantages of each biometric technique.

- *Physiological authentication*. It is seen that physiological biometrics can overall provide higher authentication accuracy than behavioral biometrics, but physiological authentication is usually one-off and requires additional hardware. For certain biometrics such as iris and retina recognition, the hardware is very expensive to deploy. Most of physiological biometrics such as fingerprint, face and hand recognition are widely accepted by users.
- *Behavioral authentication*. In contrast, behavioral biometrics can offer continuous and transparent authentication and do not require additional hardware. Thus, behavioral authentication is generally cheaper than physiological authentication. However, the accuracy of behavioral authentication is often inconsistent and would be greatly affected by users' behaviors. For example, it is hard for users to always keep performing their signature, keystroke and touch in a consistent way.

Overall, it is essential to evaluate a biometric authentication according to multi factors such as simplicity, cost, efficiency, accuracy, as well as social acceptability. Each technique has

TABLE V
EMPIRICAL EVALUATION OF DIFFERENT BIOMETRICS BASED ON THE SEVEN CHARACTERISTICS IN COMMON SCENARIOS

Biometrics	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvention**
Fingerprint	Medium	High	Medium	Medium	High	High	Medium
Face recognition	High	Low	Medium	High	Low	High	Low
Iris/retina recognition	High	High	High/Medium	Medium/Low	High	Low	High
Hand recognition	Medium	Medium	Medium	High	Medium	Medium	Medium
Palm vein recognition	Medium	High	High	Medium	High	Low	High
Voice recognition	Medium	Low	Low	High	Low	High	Low
Signature recognition	Low	Low	Low	High	Low	High	Low
Gait recognition	Medium	Medium	Low	Medium	Low	Low	Medium
Behavior profiling	High	Low	Low	High	Low	Medium	Medium
Keystroke dynamics	High	Medium	Low	High	Low	High	Medium
Touch dynamics	High	Medium	Low	High	Low	Medium	Medium

its own merits and weaknesses, thus, when implementing any biometric authentication, it is recommended to bear in mind its disadvantages and optimize its advantages.

C. Evaluation Metrics

In order to evaluate a biometric user authentication system, this section we summarize several widely accepted and used metrics as below:

- *False acceptance rate (FAR)*: indicates the possibility of identifying an impostor as a legitimate user.
- *False rejection rate (FRR)*: indicates the possibility of identifying a legitimate user as an impostor.
- *Receiver operating characteristic (ROC)*: this is a visual characterization of the trade-off between the FAR and the FRR (e.g., a graphical plot).
- *Equal error rate (EER)*: shows that the proportion of false acceptances is equal to the proportion of false rejections. The EER can be easily obtained from the ROC curve and is used to compare the accuracy of devices with different ROC curves. Generally, the lower the equal error rate, the higher the accuracy of a biometric system.
- *Authentication accuracy*: indicates the possibility of correctly identifying an individual (including both impostors and legitimate users).

In addition, biometric technologies could also be evaluated by means of the following *seven* characteristics:

- *Universality*: every person should have the biometrics.
- *Uniqueness*: no two persons are expected to have such identical biometrics.
- *Permanence*: the biometrics should not vary with time.
- *Collectability*: the biometrics should be easily collected and measurable.
- *Performance*: the accuracy of the biometrics should be stable under varied environmental circumstances.
- *Acceptability*: common users should widely accept the sample collection of the biometrics.
- *Circumvention*: the biometrics should be difficult to deceive and fool.

In Table V, we present an empirical evaluation of different biometric technologies based on three major sources:

- *Literature*. We collect existing references regarding the evaluation from the literature such as [98] and [205].
- *Online sources*. We further collect relevant information from the websites such as *biometrics.pbworks.com* and *globalsecurity.org*.
- *Our own experience*. Based on the collected information above, we then discuss and decide the final results based on our own experience.

Since the information may be a bit different from the above sources, our basic methodology is to confirm the common ones and discuss the dissident items. The differences are mainly derived from the concrete context, therefore, our evaluation results are based on common scenarios (e.g., civil use). It is worth noting that the evaluation results in Table V are only for reference, some results should be fine-tuned in a more specific environment. For example, the acceptability of voice recognition is *high* in common scenarios, but it is usually unacceptable in an environment required for high security.

On the whole, physiological biometrics provide an overall better performance due to their uniqueness as compared to behavioral biometrics, but physiological biometrics like iris recognition may require more powerful scanners, in which the cost is much higher. Although behavioral biometrics appear to perform in a less stable manner, they could provide continuous and transparent authentication to make up the shortcomings of physiological biometrics. Therefore, an appropriate combination of these two kinds of biometric techniques should be considered as a promising solution to enhance the performance of biometric user authentication.

III. ADVERSARIAL TECHNIQUES AND COUNTERMEASURES

In this section, we present a generic biometric authentication system on mobile phones, characterize eight potential vulnerable points for such a system, describe adversarial techniques and practical attacks and introduce promising countermeasures on mobile phones.

A. Generic Biometric Authentication System and Potential Attack Points

In Fig. 1, we describe a framework regarding the main logical blocks of a generic biometric user authentication system. In short, there are three major phases. The first phase is to capture biometric signals from the user. The second phase is to extract corresponding biometric features and generate templates (or patterns). The last phase is to match the generated template with the stored template and output the authentication results

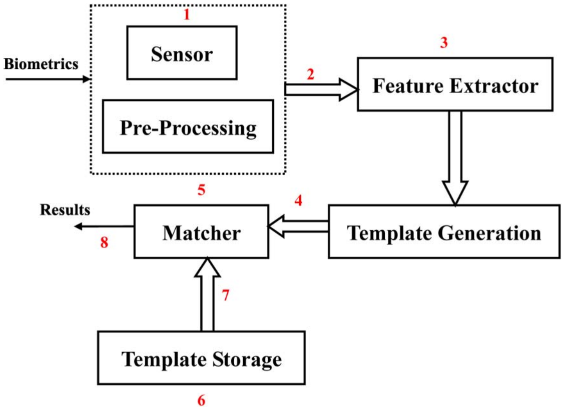

Fig. 1. Main logical blocks of a generic biometric authentication system on mobile phones (potential vulnerable points with numbers).

(or scores) (i.e., identifying as impostors or legitimate users) by considering geometry, lighting, and other signal acquisition variables during the authentication.

User authentication is often conducted based on a similarity comparison between two templates: a reference template stored in the system that was acquired during the enrolment and a new acquired template provided by the user at the point of authentication. Each time, a new template is fed into the system by extracting defined features and is then subsequently compared to the reference template. The comparison is usually performed by an algorithm while the distinctiveness in the two templates varies among different biometric techniques, especially between behavioral and physiological biometrics.

Based on [168], we identify and characterize *eight* potential attack points (or vulnerable points) with numbers for a generic biometric authentication system as shown in Fig. 1:

1) *Faking the sensor*. This type of attacks is able to conduct a possible reproduction of the biometric features as an input to the system, including a fake finger, a copy of a signature, or a face mask, etc.
2) *Resubmitting biometric signals*. This mode of attacks can bypass the sensor by replaying a previously recorded signal to the system (i.e., presenting an old copy of a fingerprint image).
3) *Overriding the feature extractor*. This mode of attacks can compromise the feature extractor and produce features which are selected by an impostor.
4) *Tampering the biometric features*. This mode of attacks can replace the transmitted features with a fraudulent feature set.
5) *Compromising the matcher*. This mode of attacks is able to compromise the matcher and utilize it to output an expected result (or score).
6) *Tampering the stored templates*. This mode of attacks can modify the templates in the database (i.e., templates are often stored in a smartcard).
7) *Attacking the channel between the stored templates and the matcher*. This type of attacks is able to intercept and modify the data exchanged through this channel.
8) *Overriding the final decision*. This mode of attacks can override the final decision which can disable the whole authentication system.

Discussions: On mobile phones (especially touch-enabled mobile phones), *templates* are possibly stored in a SIM card so that the attacks above are feasible under this framework. To mitigate these potential attacks, a biometric system can take several general countermeasures as follows:

- Adding more features to secure the sensor (i.e., adding fingerprint pulse for such recognition).
- Using cryptography to establish a more secure channel.
- Storing the data in a more secure location.

B. Practical Attacks

In this section, we present and summarize different practical attacks targeted for biometric user authentication on (touch-screen) mobile phones or similar mobile devices.

Attacks on Physiological Biometrics:

Attacks on fingerprint: To fake the fingerprint recognition, some types of attacks are feasible such as brute force attack, latent print attacks and replay attacks. For instance, Zhang *et al.* [236] presented a fingerprint attack against touch-enabled devices. The first step was to dust the touch screen surface to reveal fingerprints, and use an iPhone camera to carefully photograph fingerprints while striving to remove the virtual image of the phone from the fingerprint image. The second step was to sharpen the fingerprints in an image via image processing techniques and use algorithms to automatically map fingerprints to a keypad aiming to infer tapped passwords. In the experiments, they showed that this fingerprint attack was effective in inferring passwords from fingerprint images from iPad, iPhone, and Android phones.

Attacks on face recognition: It has been widely aware that existing face recognition systems are susceptible to fake face attacks. Duc and Minh [67] showed that fake faces like photos and video playbacks were not only easy to obtain and launch, but also quite effective to cheat a face recognition system by appropriately editing the lighting and viewpoint. Then, Li *et al.* [133] examined real-world face-authentication systems designed for smartphones, tablets, and laptops under the spoofing attacks. In the user study, their results indicated that due to online social network-based facial disclosure, the average percentage of vulnerable users for smartphone/tablet-based systems and laptop-based systems could reach 93% and 64%, respectively. Later, Erdogmus and Marcel [73] examined different types of face spoofing attacks for 2D, 2.5D, and 3D face recognition and revealed that all these recognition systems were vulnerable to spoofing attacks using facial masks.

Attacks on iris/retina recognition: To directly attack this kind of recognition systems, Ruiz-Albacete *et al.* [175] studied the direct attacks using fake iris images from real iris database. In particular, they first printed iris images with a commercial printer and then presented the images to the iris sensor. Their results showed that nearly 40% of the fake images could pass through the segmentation and normalization stages.

Attacks on Behavioral Biometrics:

Attacks on voice recognition: Some attacks have been studied against voice recognition systems such as playback attacks, speaker-adapted speech synthesis, voice conversion and

TABLE VI
THE PRACTICAL ATTACKS ON MOBILE PHONES WHICH CLAIMED BY LITERATURE

Biometric	Works	Attacks	Best Successful Rate (%)
Fingerprint recognition	[236] in 2012	Fingerprint attacks using Oily residues	63.3 (iPhone 4s)
Face recognition	[67] in 2009	Spoofing attacks	-
	[133] in 2014	Spoofing attacks	-
Iris recognition	[175] in 2008	Spoofing attacks	40 (dataset)
Voice recognition	[117] in 2012	Spoofing attacks	17.33
Keystroke and touch dynamics	[190] in 2011	Synthetic attack	-
	[146] in 2013	Mimic attacks	> 42
	[10] in 2010	Smudge attacks	68 (HTC G1/Nexus)
	[29] in 2011	Sensor-sniffing attacks	-
	[31] in 2012	Keystroke inference attack	65 (HTC Evo and Samsung Galaxy Tab)
	[148] in 2012	Keystroke inference attack	TapPrints >80 (Nexus S and iPhone 4)
	[123] in 2010	Timing attacks	- (iPhone)
	[139] in 2011	Accelerometer side channel attacks	(sp)iPhone 80 (iPhone 4)
	[158] in 2012	Accelerometer side channel attacks	ACCessory 59.6
	[11] in 2012	Accelerometer side channel attacks	43 (iPhone), 73 (Android Phone)
	[29] in 2011	Gyroscopic side channel attacks	TouchLogger 70 (HTC Evo)
	[226] in 2012	Gyroscopic side channel attacks	TapLogger 70 (HTC ADR6300)
	[90] in 2012	Location inference attacks	- (iPhone 4)

human voice mimic. For example, Kinnunen *et al.* [117] studied the vulnerability of text-independent speaker verification systems against voice conversion attacks using telephone speech. They described that the FAR of voice conversion attacks is ranged from 3.24% to 17.33%, even for the most reliable joint factor analysis (JFA) recognizer. Beranek [21] then gave a security analysis of voice biometric and identified its vulnerability.

Attacks on signature recognition: Several attacks are proved to be feasible such as hill-climbing attacks (where an impostor gradually modify the input), template attacks (where an impostor forges a signature template and shows to the recognition system) and concatenative attack (where strokes were concatenated from the corpus to build the correct passphrase). For example, Shirazi *et al.* [197] evaluated the 3D magnetic signature authentication under video-based shoulder surfing attacks and found that the magnetic gestural signature authentication was more secure than PIN-based and 2D signature methods.

Attacks on keystroke dynamics: This kind of recognition systems is vulnerable to statistic attacks, time attacks [200] and mimic attacks, in which an impostor is assumed to have access to the victim's typing statistics. For instance, Serwadda *et al.* [190] proposed a synthetic impostor attack for the keystroke dynamics-based authentication by using only general information about human typing habits. To conduct this attack, they designed *Master-key*, a probabilistic keystroke attack tool that was trained on real typing data. In the experiment, they showed that regardless of password length, there existing a category of users whose keystroke templates are critically vulnerable to an intelligent synthetic attack even for a highly restrictive online system which permits only a few false password submissions. Later, Zhuang *et al.* [240] presented an attack taking as input a 10-minute sound recording of a user typing English text by means of a keyboard and showed that up to 96% of typed characters could be recovered. This attack is a combination of machine learning and speech recognition techniques, including cepstrum features, Hidden Markov Models, linear classification, and feedback-based incremental learning. Later, Rahman *et al.* [167] conducted several experiments to verify the resilience of keystroke dynamics-based systems against non-zero effort impostor attacks (reply attacks). The experimental results showed that their attacks could drastically increase the pass-success rates from 58.99% to 87.75% using as few as 50 to 200 snooped keystroke timings.

More recently, Meng *et al.* [146] developed a feedback and training interface named *Mimesis*, which allows one person to imitate another through incremental adjustment of typing (keystroke) patterns. The experiment with 84 participants showed that if attackers have an incomplete model of the typing pattern, the success rate is around 0.52 after imitation training while for the best attackers, imitation training increases the FAR to nearly 1 (actually 0.99).

Attacks on touch dynamics: The attacks targeted for the touch dynamics-based authentication systems are similar to keystroke dynamics such as statistic attacks, mimic attacks and probabilistic touch behavioral attacks. In addition, side channel attacks including gyroscopic side channels and accelerometer side channels are a big threat for kestroke/touch dynamics. For instance, Cai *et al.* [29] described a side channel of *motion* on touch-enabled smartphones with only soft keyboards to learn users' input. To demonstrate this attack, they developed TouchLogger, an Android application that extracts features from device orientation data to infer keystrokes. Their results showed that in controlled environments, TouchLogger was able to correctly infer more than 70% of the keys typed on a number-only soft keyboard. Xu *et al.* [226] explored the feasibility of inferring a user's tap inputs to a smartphone with its integrated motion sensors. For demonstration, they further presented the design and implementation of *TapLogger*, a trojan application for the Android platform, which could stealthily log the password of screen lock and the numbers entered during a phone call.

Later, Aviv *et al.* [11] showed that the accelerometer sensor can also be employed as a high-bandwidth side channel and demonstrated how to use it to learn user tap- and gesture-based input as required to unlock smartphones using a PIN/password or Android's graphical password pattern. In the experiments, when selecting from a uniform test set of 50 possible PINs or patterns, their prediction model can predict the PIN entered

43% and pattern 73% of the time within 5 guesses on average. Moreover, the use of a touchscreen also suffers from smudge attacks [10], which attempt to extract sensitive information about the recent user input based on residual oils on touch-enabled devices. It is worth noting that smudge attacks are different from the work [236] in that the latter attempts to reveal a fingerprint (spoofing attack), while the former aims to obtain the track of the touch inputs.

Discussions on practical attacks: In Table VI, we summarize some practical attacks and successful rate claimed by literature. It is well-known that fingerprint and face recognition are vulnerable to spoofing attacks (or fake attacks). Adler [2] showed that a fairly high quality image of a person can be automatically regenerated from face recognition templates, so that biometric templates and biometric match scores should not be made available to untrusted parties.

For keystroke and touch dynamics, side channel attacks using sensors are a big threat. For example, Marquardt *et al.* [139] presented that an application with access to accelerometer readings on a modern mobile phone can use such information to recover text entered on a nearby keyboard with a rate of 80%. Their approach detects and decodes keystrokes by measuring the relative physical position and distance between each vibration. Then, Owusu *et al.* [158] showed that accelerometer readings were a powerful side channel that could be used to extract entire sequences of entered text on a smartphone touchscreen keyboard. The results presented that accelerometer measurements can be used to extract 6-character passwords in as few as 4.5 trials. Later, Templeman *et al.* [211] revealed that sensors could be used to steal information from the physical environment and introduced a 'visual malware' called *PlaceRaider*, which allows remote attackers to engage in remote reconnaissance. To defend against these attacks, it is an urgent task to design sensing management systems on the existing commodity smartphone platforms.

However, it is noted that not all side channel attacks are effective for current mobile phones. For example, key logging sound based-side channels like [12], [240] are ineffective on mobile phones with soft keyboards, as this kind of attacks requires to record and differentiate the sound emanated by different keys. In addition, Vuagnoux and Pasini [216] described that keyboards could emit electromagnetic waves which may lead to a full or a partial recovery of the keystrokes. They then proposed to acquire the raw signal directly from the antenna and to process the entire captured electromagnetic spectrum. Similarly, this attack is not functional for soft keyboards.

Moreover, due to the increase of mobile market, attackers are bound to identify the weaknesses of mobile phones and exploit them for malicious use [127], [189]. In the year of 2004, Dagon *et al.* [47] had presented a taxonomy of attacks against mobile phones and identified malware would become a key issue. Till now, malware such as virus, worms, Trojans and spyware has already become a big threat to the security and privacy of mobile phones [51], [219]. Xu *et al.* [225] explored some video-based vulnerabilities in 3G smartphones and presented a video-based spyware, called Stealthy Video Capturer (SVC), which could secretly record video information for the third party and greatly compromise users' privacy. Later, Damopoulos *et al.* [48] designed a stealth and airborne malware namely iSAM, which is able to wirelessly infect and self-propagate to the iPhone devices. Meanwhile, Schlegel *et al.* [185] presented *Soundcomber*, a Trojan with few and innocuous permissions, which could extract targeted private information from the audio sensor of mobile phones. Xing *et al.* [224] described a type of security-critical vulnerabilities, called *Pileup flaws*, through which a malicious application can strategically declare a set of privileges and attributes on a low-version operating system (OS) and wait until it is upgraded to escalate its privileges on the new system.

Malware detection has been well studied in literature, thus, it is out of the scope of this paper and we do not aim to provide a comprehensive survey here. More details related to mobile malware can be referred to malware analysis such as [53], [122] and the recent surveys regarding mobile security [125], malware propagation modeling [166] and evolution [204], [242]. Malware detection framework on mobile phones can be referred to some reports such as [238] and [239].

C. Potential Countermeasures and Discussions

Countermeasures for Physiological Biometrics: Since physiological biometrics were based a person's physical characteristics such as fingerprint, face, iris and hand, a major threat is that an impostor can replay the images of these physical characteristics to deceive the sensor. In order to enhance the authentication process of physiological biometric authentication, there are three general ways:

- *Adding features*: it is a promising method to involve more features for physiological biometrics, e.g., face recognition with eye [86], or eyeblink [161] or teeth [116]. For another example, when verifying a fingerprint, the sensor can also consider the finger pulse which can further improve the authentication accuracy [134].
- *Combining with other biometrics*: it is a promising way to combine the physiological biometrics with the behavioral biometrics to improve the authentication accuracy such as the combination of face and iris [60], face and hand [174], and face with voice [113].
- *Combining with non-biometrics-based techniques*: it is also encouraging to improve the authentication accuracy through combining physiological biometrics with non-biometrics-based techniques such as password-based authentication and token-based authentication [59].

Specific solutions: For instance, in order to overall protect mobile fingerprint templates, Hu [92] proposed several solutions such as direct biometric key generation, fuzzy fingerprint vaults and transformed biometric features. The first two solutions do not need to store fingerprint templates on smartcard, while the transformed biometric (or called cancelable fingerprint template) is to use noninvertible (cancelable) transforms to transform biometrics into a new domain where authentication is conducted. More details about cancelable fingerprint templates and fuzzy fingerprint vaults can be referred to [5], [128], [169], and [223] respectively.

To defend against spoofing attacks, biometric liveness detection has been developed. For instance, Kollreider *et al.* [119]

proposed an approach to enhance a biometric authentication framework by adding liveness awareness in a non-intrusive manner. The proposed system uses a lightweight novel optical flow, which is especially applicable in face motion estimation based on the structure tensor and inputs of a few frames. Some other related works can be referred to face liveness detection [118], [160] and fingerprint liveness detection [63]. A security evaluation regarding real spoofing attacks can be referred to [23]. In addition, electrocardiogram (ECG) signals are also discovered to prevent spoofing attacks, which are the electrical representation of the heart, due to the uniqueness of its characteristics [198]. The ECG technique can integrate with liveness detection and significantly improve the performance of liveness detection.

In addition, research has started to explore some relevant aspects that can affect the authentication performance such as how users employ and use their smartphones [17], what is the effect of their attitudes on authentication [102], and how to process data with low resolution cameras [66]. A laboratory study then can be seen in [214], which provided observations of user actions, strategies, and reactions to the authentication methods like voice and face.

Countermeasures for Behavioral Biometrics: Behavioral biometrics are mainly based on the ways people do things such as talking, signing their names and typing on keyboard/touchscreens. A major threat is that an impostor is able to mimic a person's behavior by direct or indirect observation (i.e., watching a captured video). In order to enhance the authentication of behavioral biometric authentication, there are three similar ways:

- *Adding Features*: there are many features can be extracted from a person's behavior to enhance authentication like pressure features [176], as it is very hard for an impostor to fully imitate a person's habits. For example, Zhao *et al.* [237] presented an approach of combining touch traces with pressure features to authenticate users on mobile devices. Wolf [221] described an approach of combining different sensor data such as acceleration, keystrokes and touch interactions for authenticating users. Later, Tasia *et al.* [210] showed that the performance of keystroke dynamics could be greatly promoted by adding the size and the pressure features.
- *Combining with other biometrics*: it is the same that the authentication performance can be further improved by combining the behavioral biometrics with the physiological biometrics like the combination of fingerprint and voice [24], face and voice and signatures [150], teeth and voice [115], face and teeth and voice [114].
- *Combining with non-biometrics-based techniques*: it is widely aware and accepted that the authentication accuracy can be greatly enhanced by combining behavioral biometrics with password- or token-based authentication. For example, De Luca *et al.* [61] proposed an approach of using both input patterns and the way they perform an action for authenticating users. Sae-Bae *et al.* [179] then proposed an approach of combining biometric techniques with gestural input on the multi-touch surface to verify users and could achieve an accuracy of 90%. Shahzad *et al.* [192] then proposed *GEAT*, a gesture-based user authentication scheme for the secure unlocking of touch screen devices. Ohana *et al.* [159] proposed to combine biometrics with hardware keys for secure authentication. Sun *et al.* [207] then designed a two-factor authentication system called *TouchIn*, which combined passwords with behavioral biometrics on multi-touch mobile devices.

Specific solutions: In order to improve the performance of voice recognition, Johnson *et al.* [101] developed a Vaulted Verification protocol to address the instabilities and preserves privacy of voice biometric authentication.

To detect impostors regarding behavior profiling, it is noted that anomaly detection techniques could be utilized. For instance, Schmidt *et al.* [187], [188] demonstrated how to monitor a Symbian smartphone to extract features, which can be used for anomaly detection. In reality, anomaly detection is often applicable for behavioral biometric authentication after building a normal profile of user's behavior.

In order to enhance the performance of keystroke dynamics-based authentication, Monrose *et al.* [151] proposed a method of combining user's normal typing patterns (e.g., durations of keystrokes and latencies between keystrokes) with the user's password to generate a *hardened password*, which is convincingly more secure than the traditional passwords. Bergadano *et al.* [20] described a measure for keystroke dynamics that limits the instability. They tested the approach with 154 persons and achieved a false alarm rate of about 4% and an impostor pass rate of less than 0.01%. Then, Stefan *et al.* [203] evaluated the security of keystroke dynamics-based system against synthetic forgery attacks and designed a framework called *TUBA* for monitoring users' typing patterns.

With the advent of touchscreens, keyboard can be classified as hardware keyboard and software keyboard. For instance, Draffin *et al.* [69] proposed a passive authentication method by modeling the micro-behavior of users' interaction with their devices' software keyboard. They show that the way a user types such as the specific location touched on each key, the drift from finger down to finger up, the force of touch and the area of press, can construct the unique physical and behavioral characteristics. The results showed that their approach could passively identify that a mobile device was being used by a non-authorized user within 5 key presses 67.7% of the time. Later, Park *et al.* [164] investigated the effects of touch key sizes and locations on the one-handed thumb input in mobile phone interactions, and provided how to design touch keys.

To prevent smudge attacks, AlRowaily and AlRubaian [3] presented WhisperCore, a system that requires the user to wipe parts of the screen at the end of the login procedure to mask the smudge of the actual authentication with a new smudge trail. Later, Schneegass *et al.* [184] presented SmudgeSafe, an authentication system that used random geometric image transformations, such as translation, rotation, scaling, shearing, and flipping, to disturb users inputs.

In addition, some efforts have been made to remotely wipe sensitive data for the stolen smartphones. For example, Yu *et al.* [232] proposed a remote deletion mechanism that allowed the phone owners to delete their private data remotely even if WiFi is disabled and SIM card is unplugged. The basic idea is to utilize emergency call mechanisms to establish a communication connection with a service provider to verify the state of the phone and perform remote deletion. Several related anti-theft schemes can be seen in [99], [202], and Apple has already provided *Find My iPhone* for users [8].

Discussions on countermeasures: Many studies and experiments such as [39], [93] have shown that the use of a single biometric may be not enough to provide reliable user authentication. In order to improve authentication performance, it is noted that different biometrics could be combined appropriately, which called *multimodal biometrics*. The *multimodal biometrics* can be defined as:

- Systems that are capable of using more than one physiological or behavioral characteristic for enrollment, verification and identification.

The countermeasures mentioned above like *combining with other biometrics* and *combining with non-biometrics-based techniques* are two ways of realizing *multimodal biometrics* on mobile devices like mobile phones. Many efforts have been conducted in literature. For example, Hazen *et al.* [91] proposed a multimodal by combining face and speaker identification on mobile devices. Then, Angulo and Wästlund [6] presented a two-factor authentication system of combining graphical passwords with touch gestures on mobile phones. They involved 32 participants and their experiments on Android phones demonstrated that an EER of 10.39% could be achieved. Later, De Marsico *et al.* [60] described FIRME (Face and Iris Recognition for Mobile Engagement) as a biometric application based on a multimodal recognition of face and iris, which was designed to be embedded in mobile devices.

It is widely well-recognized [178] that constructing a multimodal biometrics-based authentication can often improve the performance of a single biometrics-based authentication, and achieve a higher and more consistent authentication accuracy. However, a fundamental problem is how to implement the multimodal biometric authentication in an appropriate way; otherwise, attacks are still feasible [23]. This aspect is considered in the next section.

IV. Secure Biometric User Authentication Mechanism

In this section, we characterize a framework for establishing a secure multimodal authentication mechanism, and present a study of implementing the authentication mechanism regarding touch dynamics.

A. Authentication Mechanism

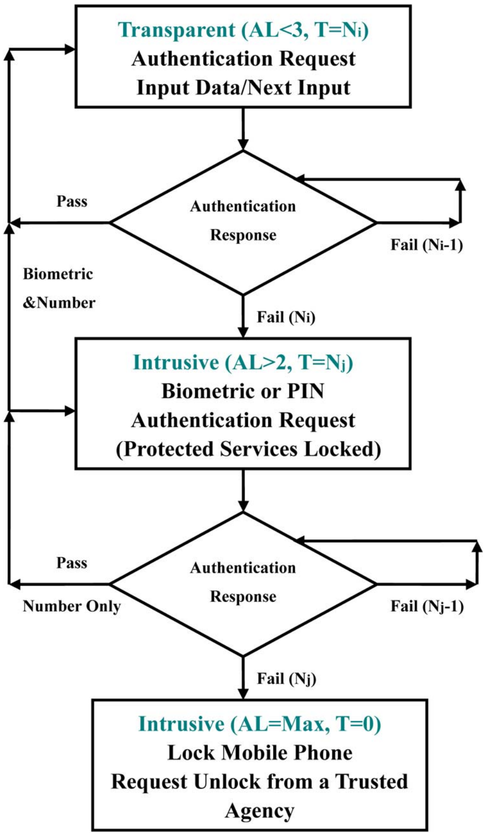

Fig. 2. A framework of establishing a reliable authentication mechanism on mobile phones.

Many research studies like [178] have pointed out that no single biometric approach is ideally suited to all scenarios, and that multimodal biometric approaches are often superior to single biometric methods. In this case, multimodal biometrics are expected to provide more reliable authentication performance, but a reliable/successful authentication mechanism is required to guarantee implementing the multimodal biometric user authentication in an appropriate way. What is more, a successful authentication mechanism on mobile phones should meet several objectives as below:

- Increasing authentication security beyond secret knowledge based approaches (e.g., PIN).
- Providing transparent authentication aiming to remove the inconvenience factor.
- Providing continuous and periodic authentication of the user rather than a one-off authentication.
- Providing a workable architecture across the different OS platforms of mobile phones.
- Requiring or increasing affordable workload on mobile phones. Overhead is an important factor which can affect the battery lifetime.
- Providing appealing usability for users letting them be willing to adopt this authentication mechanism.

In Fig. 2, we characterize a framework for establishing a reliable authentication mechanism on mobile phones from the literature works like [44]. To implement a reliable authentication mechanism, multi-level authentication is desirable to comprehensively assess a person aiming to reduce authentication errors (or uncertainty). Our characterized framework can provide multi-level authentication and is also suitable for other mobile devices. The framework enables the multimodal biometrics-based authentication using a combination of both non-biometric and biometric techniques. Three specific security measures are developed as follows:

- *Alert level (AL)*: indicates the security level of current authentication states.
- *Tolerance number (T)*: indicates the number of failed authentication attempts that can be affordable within an alert level.
- *Actions and responses*: indicate the corresponding actions to either a successful or a failed authentication.

Mechanism Discussions: The objective of multimodal authentication mechanism as shown in Fig. 2 is to provide a secure user authentication through combining either biometrics-based or non-biometrics-based techniques. That is, the multimodal authentication framework can include biometrics like physiological or behavioral biometrics and non-biometrics like PIN during user authentication.

The major reason for combining both biometrics and non-biometrics in the multimodal mechanism above is that they can complement to each other. For instance, PIN can only provide one-off authentication while biometrics can offer continuous and transparent authentication. By contrast, biometrics are impossible to change but a PIN can be easily updated based upon users' demands. We also notice that current mobile providers, such as Apple, employ both biometrics and non-biometric methods in their mobile device authentication (i.e., the iPhone 5s employs both fingerprint recognition and PIN). In these cases, the use of PINs and passwords are currently retained as the last line of defense, when biometric authentication may not work (i.e., it is hard to authenticate in the dark using the face recognition, fingerprint approaches may not function in the rain, etc.) [22]. Thus, in Fig. 2, we also retain the PIN within the framework for similar reasons.

Practical Implementation: In order to explain and deploy the framework in practice, we present an example in Fig. 3 that includes 4 alert levels. It is noted that for current commercial mobile authentication mechanisms, most multimodal biometrics would deploy PIN as the final defense line for authentication. For example, Apple phones like iPhone 5s include a multimodel biometrics-based authentication by combining fingerprint and PIN, while the phone requires the users to enter password after five unsuccessful match attempts. The objective of this mechanism is to balance both security and usability. Therefore, we adopt this piratical authentication mechanism in Fig. 3 and the concrete authentication process can be described into three stages.

- At the first stage, the alert level (AL) is set to 1 and the tolerance number (T) is set to 2. In this case, users have up to 2 attempts during the authentication and they can pass the authentication as long as one input is successful. However, if all attempts are failed, then the authentication system will enter the next stage.
- At the second stage, the alert level is increased to 2 and the tolerance number is decreased to 1. In addition, some protected services may be locked under this stage. If users input correctly, then the authentication system can go back to the first stage; otherwise, the system will enter the third stage.
- At the third stage, users are initially treated as impostors by default (where AL is 3 and T is 1), thus, they have to input both PIN and biometric information.
  - — If both information is correct, then the authentication system can go back to the first stage whereas the system can only go back to the second stage if only PIN is correctly input.
  - — If no any information is correct, the authentication system will lock the mobile phones and require an administrator to unlock it.

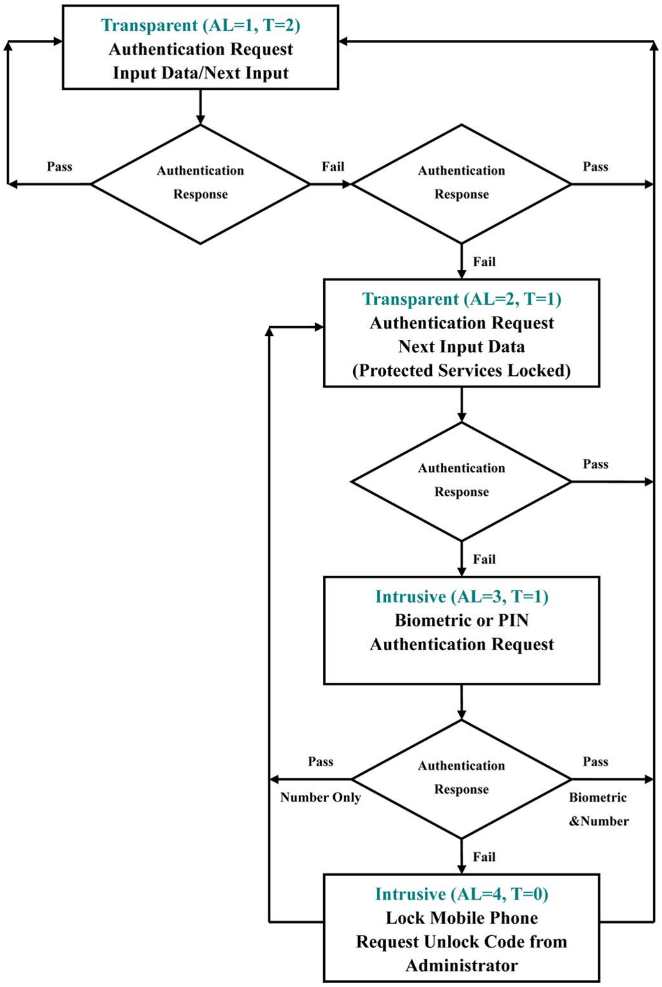

Fig. 3. An example of the reliable authentication mechanism showing the response to failed authentication attempts.

Discussions: The performance of the authentication mechanism above usually depends heavily upon the employed biometric techniques on particular mobile phones. For example, if we employ face recognition and PIN in the authentication process shown in Fig. 3, then the corresponding FRR and FAR can be represented as:

$$FRR = FaceRec_{FRR} \times FaceRec_{FRR} \times FaceRec_{FRR} \times PIN_{FRR}$$

$$FAR = FaceRec_{FAR} \times FaceRec_{FAR} \times FaceRec_{FAR} \times PIN_{FAR}$$

```
V/Action Down(  164): Action Down:
Press time is 1090828
V/Action inputdevice(  164):
x=122.7138,y=588.37286,pressure0.090
19608,size=0.06666667
I/InputDevice(  164):
x=122.7138,y=588.37286,pressure0.090
19608,size=0.06666667
V/Action inputdevice(  164):
x=126.11902,y=581.70825,pressure0.10
1960786,size=0.06666667
I/InputDevice(  164):
x=126.11902,y=581.70825,pressure0.10
1960786,size=0.06666667
V/Action inputdevice(  164):
x=133.05556,y=568.37897,pressure0.12
156863,size=0.06666667
I/InputDevice(  164):
x=133.05556,y=568.37897,pressure0.12
156863,size=0.06666667
V/Action inputdevice(  164):
x=143.64955,y=552.6605,pressure0.121
56863,size=0.06666667
I/InputDevice(  164):
x=143.64955,y=552.6605,pressure0.121
56863,size=0.06666667
V/Action inputdevice(  164):
x=157.64876,y=530.026,pressure0.1254
```

(a) (b)

Fig. 4. Google/HTC *Nexus One*. (a) Android phone interface. (b) Raw data collection.

In this case, various levels of authentication performance could be achieved by employing different biometrics within the authentication mechanism (i.e., replacing the face recognition with other biometrics).

B. Practical Study

Since touch dynamics becomes much prevalent in current touchscreen mobile phones, in this section, we conduct a practical study regarding touch dynamics-based authentication based on Fig. 3. This effort attempts to drive more research efforts regarding this emerging biometric technique.

As mentioned above, we employ PIN in the study as the last defense line to authenticate users. There are two major reasons to choose it: one is that this kind of authentication mechanisms is very popular in practical mobile phone authentication like iPhone 5s, while the other is that PIN is widely accepted by users. In addition, by employing PIN, we can compare and discuss the authentication performance with and without it.

Implementation details: To implement the authentication above, we used a Google/HTC *Nexus One* Android phone with a multi-touch capacitive touchscreen (resolution 480 × 800 px) to collect and process data. The CPU of this particular phone is 1 GHz while the storage memory is 512 M. We updated the phone with a modified Android OS based on *CyanogenMod*.[3] The modification consists of changes to the application framework layer to record raw input data from the touchscreen, such as the timing of touch inputs, the coordinates, the types of the input (e.g., press down, press up) and the touch pressure. In addition, we installed a separate application to help extract the recorded data from the phone.[4] In Fig. 4, we present the interface of Google/HTC *Nexus One* and show an example of raw data captured by the log application. More details of the implementation can be referred to [143]–[145].

TABLE VII
RESULTS FOR TOUCH DYNAMICS-BASED AUTHENTICATION UNDER THE AUTHENTICATION MECHANISM

Authentication Method	Practical Average FRR/FAR at 1st Stage (%)	Expected Average FRR/FAR at Last Stage (%)
Our practical study	4.76/3.82	0.0000431/ 0.0000223

Feature selection: Based on our previous experience [143], [144], we propose a new scheme in this study which employs 22 touch related features such as *average touch movement speed per direction (8 directions)*, *fraction of touch movements per direction (8 directions)*, *average single-touch time*, *average multi-touch time*, *the number of touch movements per session*, *the number of single-touch events per session*, *the number of multi-touch events per session* and *touch pressure*.

Algorithm selected and user involved: A hybrid algorithm of PSO-RBFN (Particle Swarm Optimization+Radial Basis Function Network) [143] is used for the user authentication. A total of 80 users joined our study and all participants are regular mobile phone users who are ranged in the age from 16 to 55 years, including 42 males and 38 females. Among these participants, 70 percent of them were students while the others are senior citizens, engineers and businessmen.

Data collection: For collecting data, we provided all the participants with an Android phone equipped with our modified Android OS and asked participants to use the phones the same way they would use their own phones in their normal lives, such as browsing websites, accessing files and operating on any applications. In addition, all participants are requested to complete 25 sessions within 3 days when they are using the phone. Each session includes a total of 100 touch gestures.

The specific authentication procedure based on Fig. 3 can be described as below:

- At the first stage, authentication system can allow two failed touch related gesture-patterns. If both attempts are failed, then the system would enter the next stage $(AL=2)$.
- At the second stage, if another input gesture-pattern fails, then the system would enter the third stage $(AL = 3)$.
- At the third stage, both a correct touch related gesture-pattern and a right PIN are requested.

In [44], the FRR of PIN was set to 0.4% according to the results from the National Physical Laboratory. In this work, as a study, we adopt it and set an equal FRR and FAR of PIN authentication to 0.4%. Thus the authentication accuracy can be described in Table VII.

Result discussions: In the user study, we find that users can achieve a practical average FRR of 4.76% and average FAR of 3.82% respectively, regarding our touch dynamics-based authentication scheme on mobile phones. Therefore, under the full authentication mechanism which includes PIN authentication, the expected average FRR and FAR is 0.0000431% and 0.0000223% respectively. However, if we only employ touch dynamics-based authentication, then the FRR and FAR would increase to 0.0108% and 0.0059% respectively.

[3] http://www.cyanogenmod.com/

[4] The customized-Android OS is available from our project website at: https://sourceforge.net/projects/touchdynamicsauthentication/files/Android_OS/.

Overall, it is found that the combination of touch dynamics and PIN can indeed reduce the error rates of any single biometric alone. Compared to the results of Tables II and Table III, our study validates that the multimodal authentication mechanism can greatly improve the authentication performance of a single biometric user authentication system.

It is worth noting that the results obtained in this study only attempt to provide a reference to present the performance of multimodal authentication and to illustrate how difficult it is for an impostor to access to sensitive information under such mechanism. There do still exist several challenges and open problems, which we will discuss in Section V.

C. Discussions on Biometric Authentication Frameworks

In literature, we identify that multimodal authentication is only one of the existing biometric authentication frameworks. Therefore, in this section, we aim to summarize and discuss six typical biometric authentication frameworks on mobile phones as follows.

Biometric signature-based framework: Such framework is mainly based on the comparison of biometric signatures during the authentication. *Physiological authentication* such as fingerprint, face, iris recognition usually employs such framework since it is not hard to create a correct signature of these biometrics (these biometrics are unique and most consistent). Taking face recognition as an example, the framework would first build a correct signature for a user' face and then compare the later inputs with the correct one for authentication (see [1], [87]). The key point for this kind of frameworks is to choose proper features to describe different biometrics.

Biometric anomaly-based framework: This framework is similar to anomaly-based detection, which mostly utilizes machine learning techniques during authentication. *Behavioral authentication* often employs this framework to detect impostors. The framework should first describe the normal behaviors using appropriate features and then monitor users' behaviors for detecting deviations. If the deviation exceeds a defined threshold, then the framework will consider the current user is an impostor. For example, Damopoulos *et al.* [49] proposed an anomaly-based detection system on mobile phones to detect anomalies by monitoring users actions like Telephone call, SMS and Web browsing, and compared the performance of four machine learning classifiers.

Multimodal-based framework: This framework is widely adopted in many research works and practical implementation, since it is well known that a single biometric cannot guarantee highly reliable authentication [39]. The user study presented above demonstrates the advantages of this framework as well, in which a multimodal biometric can significantly reduce the error rates. Under this framework, several biometrics would be combined properly to provide a more reliable authentication than a single biometric, such as a combination of face and iris [60], face and hand [174], face and voice [113], password and writing signatures [111], etc. Although this framework is very popular in both academia and industry, the key point for ensuring its effectiveness is to identify specific scenarios and combine biometrics in an appropriate way.

Cloud-based framework: With the rapid development of cloud computing, it is promising for biometric authentication to offload the heavy workload to a cloud. Damopoulos *et al.* [52] argued that both host- and cloud-based detection systems can operate concurrently to complement each other and proposed a new authentication framework which decouples the IDS from where it is hosted, enabling the "movement" of mechanisms from host to cloud and viceversa transparently without any modifications to the IDS. Their architecture can support diverse anomaly-based mechanisms to be concurrently applied, either directly on the device, or by offloading computation on the cloud, maximizing synergy between device and cloud-hosted defenses.

In addition, cloud can also be used to monitor applications' behaviors. For instance, Papamartzivanos *et al.* [162] designed a host and cloud-based synergistic mechanism for preserving mobile users' privacy, through sharing apps' behavioral profile among the participating users, and thus offer them the ability to control privacy exposures. As mobile phones usually have limited processing and memory resources compared to those of PCs, the cloud-based framework is becoming a popular alternative to offload a significant part of their operation to the cloud.

Contextual information-based framework: This framework usually integrates other factors from a scenario (called *contextual information*) to authenticate a user. For instance, Shabtai *et al.* [193] proposed a detection framework, where time-stamped security data is continuously monitored within a mobile phone. Their approach integrates many contexts such as the continuously measured data (e.g., the number of sent SMSs), the events (e.g., software installation) and the security domain knowledge-base (i.e., an ontology for abstracting meaningful patterns from raw, time-oriented security data).

Later, Shi *et al.* [196] proposed an authentication framework based on users' recent activities related to location, motion, communication and the usage of applications. Riva *et al.* [171] focused on the problem of when to surface authentication and for which applications, and proposed a mobile system that progressively authenticated (and de-authenticated) users by constantly collecting cues about the user. The key insight is to combine multiple authentication signals to determine the user's level of authenticity, and surface authentication only when this level is too low. The study results showed that they could reduce nearly half number of explicit authentications. The key point for this framework is to integrate appropriate contextual information to enhance the generated patterns.

Configurable framework: This framework enables developers and researchers to reconfigure some parameters and settings, which provides more flexibility than a fixed framework. Khan *et al.* [110] pointed out that the authentication schemes proposed by the research community are challenging to deploy, and there is a need for a framework that supports different behavioral classifiers, given that different applications have different requirements. Then, they designed *Itus*, an implicit authentication framework for Android that allows the research community to improve these schemes incrementally, while allowing application developers to determine these improvements at their own pace. In other words, developers can deploy *Itus* in an application-specific manner, adapting to their unique needs. The major advantage of this framework is its adaptiveness and scalability, which can facilitate its implementation according to different requirements.

Discussions: Overall, all these frameworks attempt to provide better security and usability for user authentication on mobile phones. It is noted that the biometric signature-based framework is straightforward relying on the uniqueness and consistence of biometrics, while the biometric anomaly-based framework usually identifies great deviations between current inputs and predefined templates. Due to these features, physiological biometrics usually employ the former and behavioral biometrics often adopt the latter. To summarize, the multimodal-based framework is very promising at improving the authentication accuracy by combining several biometrics in an appropriate way. It is well noted that multimodal-based authentication is often more reliable than a single biometric authentication.

The cloud-based framework is much useful when the authentication workload is high, as the computation can be offloaded to the cloud. In general, all the frameworks above can utilize clouds to reduce their burden and improve the efficiency. The contextual information-based framework can integrate more factors in authenticating users, where the contextual information mainly refers to environmental factors (a bit different from multimodal). The configurable framework can provide much more flexibility in implementation, which is desirable for developers and researchers.

V. Open Problems and Discussions

In this section, we identify challenges and future trends in this area, and discuss experiences learned from designing biometric user authentication on mobile phones.

A. Challenges and Future Trends

Biometric authentication attempts to verify users according to either users' physical characteristics or behavioral habits. Although this kind of authentication has been developed over twenty years, there are still many challenges and open problems when authenticating users using biometrics. From another angle, these challenges undoubtedly provide interesting and important topics for developing such kind of authentication in future. We describe these challenges as below.

Biometric feature selection: To select an appropriate set of biometric features is a big challenge for biometric user authentication. Take touch dynamics as an example, many touch related features are available such as touch movement, touch direction, touch pressure, scroll, etc. In order to design a reliable authentication mechanism, how to select, decide and optimize an appropriate set of biometric features is a challenge and an open problem.

Algorithm development: When having a set of biometric features, another challenge is how to develop an appropriate algorithm to improve or optimize the performance of authentication. Take behavior profiling as an example, the performance depends heavily on the designed algorithms that are used to generate pattern classification model. With the rapid development of computing, it is an important topic for designing more powerful algorithms for biometric authentication.

Users behavioral habit: To authenticate users by means of the behavioral biometric authentication, a big challenge is that the authentication accuracy may be greatly decreased if the user performs very differently from his/her daily inputs (i.e., increasing false rates). This is a well-known and major limitation and an open problem for degrading the performance of behavioral biometric authentication.

Involved users: To evaluate any biometric user authentication, involved users are a very important factor to affect the obtained results (i.e., different users may result in distinct patterns). Therefore, conducting a larger user study with even more users is always desirable. To enhance the evaluation, it is an important topic to explore how to conduct a *systematic* user study and experiment.

Evaluation platform: A large number of biometric user authentication schemes have been proposed in literature aiming to improve the performance of authentication. However, it lacks of widely accepted and available benchmark in this area for comparing different works. To develop a standard evaluation platform in this area is a big challenge.

Leakage-resilient input: Shoulder-surfing attacks are always a threat for user authentication, which use direct observation techniques such as looking over someone's shoulder, to get private information. Biometric authentication especially behavioral biometric authentication is vulnerable to such attacks, since an attacker can mimic users' behaviors by observation. Therefore, to design an appropriate method of leakage-resilient entry is very important like [228].

Usability limitation: Most matching algorithms for biometric authentication often operate with a high FRR at thresholds attempting to keep the FAR under 0.1% [142]. However, this unbalance may make the whole system unusable. Thus, it is a critical topic to explore how to make a balance.

Increasing attacks: With the popularity of mobile phones, more threats and attacks have been emerged. Therefore, it is a big challenge to learn how to defend against these attacks on mobile phones like liveness detection, keylogger/touchlogger detection, etc.

Future trends: Touch-enabled mobile phones will become extremely popular in future mobile market where 800 million mobile phones (50% of the total number) are expected to be touch-enabled by 2014 [129] and this percentage seems to be increasing. The use of a touchscreen can provide many new features during the interaction between the phone and the users such as touch movement and various multi-touch gestures. In addition, a touchscreen offers a promising interface for both physiological and behavioral approaches (i.e., touchscreen can verify fingerprint and touch dynamics simultaneously).

Therefore, we point out that *touchscreen mobile phones* will become a mainstream in future mobile market and can provide many appealing topics in both academia and industry, and predict that *touch dynamics* will play a more important role in future when designing a reliable biometric user authentication mechanism on mobile phones.

B. Experiences Learned Regarding Balances

Biometric authentication is considered as a promising alternative to the traditional text-based authentication, as biometrics can provide many unique characteristics. However, designing a reliable user authentication mechanism on mobile phones is not an easy task, we should learn how to make balances to achieve this goal.

Balance between cost and implementation: Intuitively, all biometrics mentioned in this work, including both physiological and behavioral biometrics, can be implemented on a mobile phone. But in practice, not all biometrics can be deployed in a mobile phone, we need to consider the balance between cost and implementation. For example, retina scan can achieve a very high authentication accuracy but the cost is too high to implement it on mobile phones, e.g., it is very expensive to develop a special scanner on phones.

Another example, hand recognition also costs a lot if deploying a scanner on phones. The reason is that a touchscreen should be big enough to scan the whole hand. However, if we use a hand image for authentication, the cost can be greatly reduced as most smartphones have a built-in camera. Overall, to develop a proper user authentication, it is very important to make a balance between cost and implementation.

Balance between overhead and performance: It is generally recognized that by integrating more biometric features, the authentication performance could be increased. In our study on touch dynamics, it is found that adding more related touch features can decrease the authentication errors. However, the major problem is that more features may cause more time and workload to collect data and compute feature values. Negatively, the added workload may slow down the authentication process, which make users dislike the authentication and give up it. Thus, it is also very important to balance overhead and performance when designing an authentication scheme.

Balance between security and usability: It is well known that a balance should be made between security and usability for a biometric system [25]. For instance, a false rejection (usability) is less costly than a false acceptance (security), since a higher false acceptance rate will lower the security level of the authentication system, while a higher false rejection rate will frustrate a legitimate user, which is still unfortunate but arguably less problematic than a lower security level.

We find that poor usability can degrade the security level (i.e., users create poor secrets) while poor security can directly harm users' privacy. Thus, it is a key balance that should be made between security and usability, when designing practical authentication schemes.

Balance between biometrics and non-biometrics: To build a reliable authentication mechanism, based on our study and real-world mobile authentication, we find that a balance should be made between biometrics and non-biometrics since these two are complementary to each other. We cannot unconditionally separate them as each of them suffers from several issues. Thus, in the proposed authentication mechanism (see Section IV), we allow to employ both biometrics and non-biometrics together aiming to provide a better authentication performance to users in the aspects of security and usability.

VI. Conclusion

In this article, we survey the development of biometric user authentication techniques on mobile phones, especially touch-enabled phones, according to physiological and behavioral approaches. Physiological biometrics are based on a person's physical characteristics while behavioral biometrics are based on a behavioral habit of an individual. By reviewing a number of related works, we identify that physiological biometrics can provide high authentication accuracy, but they usually require additional hardware and only perform a one-off authentication. On the contrary, behavioral biometrics can provide continuous and transparent authentication without additional equipments, but the accuracy is not stable enough.

Although biometric authentication is encouraging, we find that it is difficult to replace all password- and token-based authentication with biometrics. Biometric authentication still suffers from two major shortcomings: accuracy and speed. For example, most biometric systems cannot provide a FRR under 1% and it is time-consuming to register and verify biometrics if sensors are not good enough. In order to build a reliable authentication mechanism, we identify that multimodal biometric authentication is better than a single biometric system. As biometrics and non-biometrics are complementary to each other, we suggest considering both of them in a practical user authentication scheme, aiming to enhance both security and usability. It is noticed that current mobile providers, such as Apple, employ both biometrics and non-biometric methods in their mobile device authentication (e.g., iPhone 5s).

Moreover, we identify that some open problems and balances should be considered when designing biometric systems, and point out that with the development of touchscreens, touch dynamics will become more important and useful in designing future biometric authentication mechanisms on mobile phones. For instance, the use of multi-touch gestures can provide more choices to enlarge password entropy and increase the difficulty of observation and smudge attacks. We hope that this article could drive more research to investigate the challenges and open problems identified in this area.

References

[1] P. Abeni, M. Baltatu, and R. D'Alessandro, "Implementing biometrics-based authentication for mobile devices," in *Proc. IEEE GLOBECOM*, 2006, pp. 1–5.

[2] A. Adler, "Can images be regenerated from biometric templates?" in *Proc. Biometric Conf.*, 2003, pp. 1–2.

[3] K. Airowaily and M. Alrubaian, "Oily residuals security threat on smart phones," in *Proc. Int. Conf. Robot, Vis. Signal Process.*, 2011, pp. 300–302.

[4] A. A. E. Ahmed and I. Traore, "A new biometric technology based on mouse dynamics," *IEEE Trans. Dependable Secure Comput.*, vol. 4, no. 3, pp. 165–179, Jul.–Sep. 2007.

[5] R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," in *Proc. ACISP*, 2005, pp. 242–252.

[6] J. Angulo and E. Wästlund, "Exploring touch screen biometrics for user identification on smart phones," in *Proc. Privacy Identity Manage. Life*, 2012, pp. 130–142.

[7] "Apple Invents Facial Recognition Locking & Unlocking System," 2012. [Online]. Available: http://www.patentlyapple.com/patently-apple/2012/09/apple-invents-facial-recognition-locking-unlocking-system.html

[8] Apple Inc., Find my iPhone, iPad, iPod touch, or Mac., Cupertino, CA, USA. [Online]. Available: https://www.apple.com/icloud/find-my-iphone.html

[9] M. T. I. Aumi and S. Kratz, "AirAuth: A biometric authentication system using in-air hand gestures," in *Proc. CHI*, 2014, pp. 499–502.

[10] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Proc. 8th USENIX WOOT*, 2010, pp. 1–10.

[11] A. J. Aviv, B. Sapp, M. Blaze, and J. M. Smith, "Practicality of accelerometer side channels on smartphones," in *Proc. ACSAC*, 2012, pp. 41–50.

[12] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *Proc. IEEE Symp. Security Privacy*, 2004, pp. 3–11.

[13] J. Ashbourn, *Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity*. Zürich, Switzerland: Springer-Verlag, 2014.

[14] D. Bassu, M. Cochinwala, and A. Jain, "A new mobile biometric based upon usage context," in *Proc. IEEE Int. Conf. Technol. HST*, 2013, pp. 441–446.

[15] R. Blanco-Gonzalo, O. Miguel-Hurtado, A. Mendaza-Ormaza, and R. Sanchez-Reillo, "Handwritten signature recognition in mobile scenarios: Performance evaluation," in *Proc. IEEE Int. Carnahan Conf. Security Technol.*, 2012, pp. 174–179.

[16] M. Baloul, E. Cherrier, and C. Rosenberger, "Challenge-based speaker recognition for mobile authentication," in *Proc. BIOSIG*, 2012, pp. 1–7.

[17] P. Bao, J. Pierce, S. Whittaker, and S. Zhai, "Smart phone use by non-mobile business users," in *Proc. MobileHCI*, 2011, pp. 445–454.

[18] J. Baumann, "Voice Recognition." [Online]. Available: http://www.hitl.washington.edu/scivw/EVE/I.D.2.d.VoiceRecognition.html

[19] M. Becher *et al.*, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. IEEE Symp. Security Privacy*, 2011, pp. 96–111.

[20] F. Bergadano, D. Gunetti, and C. Picardi, "User authentication through keystroke dynamics," *ACM Trans. Inf. Syst. Security*, vol. 5, no. 4, pp. 367–397, Nov. 2002.

[21] B. Beranek, "Voice biometrics: Success stories, success factors and what's next," *Biometric Technol. Today*, vol. 2013, no. 7, pp. 9–11, Jul. 2013.

[22] C. Bhagavatula, K. Iacovino, S. M. Kywe, L. F. Cranor, and B. Ur, "Usability analysis of biometric authentication systems on mobile phones," in *Proc. SOUPS*, Menlo Park, CA, USA, 2014, pp. 1–2.

[23] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under realistic spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.

[24] J. Bigun, J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Combining biometric evidence for person authentication," in *Advanced Studies in Biometrics*. Berlin, Germany: Springer-Verlag, 2005, pp. 1–18.

[25] C. Braz and J.-M. Robert, "Security and usability: The case of the user authentication methods," in *Proc. IHM*, 2006, pp. 199–203.

[26] A. S. Brown, E. Bracken, S. Zoccoli, and K. Douglas, "Generating and remembering passwords," *Appl. Cogn. Psychol.*, vol. 18, no. 6, pp. 641–651, Sep. 2004.

[27] A. Buchoux and N. L. Clarke, "Deployment of keystroke analysis on a smartphone," in *Proc. 6th Australian Inf. Security Manage. Conf.*, 2008, pp. 1–7.

[28] U. Burgbacher and K. Hinrichs, "An implicit author verification system for text messages based on gesture typing biometrics," in *Proc. CHI*, 2014, pp. 2951–2954.

[29] L. Cai and H. Chen, "Touchlogger: Inferring keystrokes on touch screen from smartphone motion," in *Proc. 6th USENIX Conf. HotSec*, 2011, pp. 1–6.

[30] L. Cai, S. Machiraju, and H. Chen, "Defending against sensor-sniffing attacks on mobile phones," in *Proc. ACM Workshop Netw., Syst., Appl. Mobile Handhelds*, 2009, pp. 31–36.

[31] L. Cai and H. Chen, "On the practicality of motion based keystroke inference attack," in *Proc. Trust*, 2012, pp. 273–290.

[32] Z. Cai, C. Shen, M. Wang, Y. Song, and J. Wang, "Mobile authentication through touch-behavior features," in *Proc. CCBR*, 2013, pp. 386–393.

[33] P. Campisi, E. Maiorana, M. Lo Bosco, and A. Neri, "User authentication using keystroke dynamics for cellular phones," *IET Signal Process.*, vol. 3, no. 4, pp. 333–341, Jul. 2009.

[34] X. Chen, J. Tian, Q. Su, X. Yang, and F.-Y. Wang, "A secured mobile phone based on embedded fingerprint recognition systems," in *Proc. ISI*, 2005, pp. 549–553.

[35] S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones," in *Proc. MobiSys*, 2014, pp. 109–122.

[36] D.-H. Cho, K. R. Park, D. W. Rhee, Y. Kim, and J. Yang, "Pupil and iris localization for iris recognition in mobile phones," in *Proc. SNDP*, 2006, pp. 197–201.

[37] M. Choras and R. Kozik, "Contactless palmprint and knuckle biometrics for mobile devices," *Pattern Anal. Appl.*, vol. 15, no. 1, pp. 73–85, Feb. 2012.

[38] S. Choi, I.-H. Youn, R. LeMay, S. Burns, and J.-H. Youn, "Biometric gait recognition based on wireless acceleration sensor using k-nearest neighbor classification," in *Proc. ICNC*, 2014, pp. 1091–1095.

[39] N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds, "Acceptance of subscriber authentication methods for mobile telephony devices," *Comput. Security*, vol. 21, no. 3, pp. 220–228, Jun. 2002.

[40] N. L. Clarke, S. M. Furnell, B. M. Lines, and P. L. Reynolds, "Keystroke dynamics on a mobile handset: A feasibility study," *Inf. Manage. Comput. Security*, vol. 11, no. 4, pp. 161–166, 2003.

[41] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones—A survey of attitudes and practices," *Comput. Security*, vol. 24, no. 7, pp. 519–527, Oct. 2005.

[42] N. L. Clarke and S. M. Furnell, "Authenticating mobile phone users using keystroke analysis," *Int. J. Inf. Security*, vol. 6, no. 1, pp. 1–14, Jan. 2007.

[43] N. L. Clarke and A. R. Mekala, "The application of signature recognition to transparent handwriting verification for mobile devices," *Inf. Manage. Comput. Security*, vol. 15, no. 3, pp. 214–225, 2007.

[44] N. L. Clarke and S. M. Furnell, "Advanced user authentication for mobile devices," *Comput. Security*, vol. 26, no. 2, pp. 109–119, Mar. 2007.

[45] H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in *Proc. PST*, 2010, pp. 205–212.

[46] P. Daniel, "HTC One Max and Sense 5.5: All the New Features Review," Oct. 2013. [Online]. Available: http://www.phonearena.com/news/HTC-One-max-and-Sense-5.5-all-the-new-features-review_id48265

[47] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" *IEEE Pervasive Comput.*, vol. 3, no. 4, pp. 11–15, Oct.–Dec. 2004.

[48] D. Damopoulos, G. Kambourakis, and S. Gritzalis, "iSAM: An iPhone stealth airborne Malware," in *Proc. IFIP Int. Inf. SEC*, 2011, pp. 17–28.

[49] D. Damopoulos *et al.*, "Evaluation of anomaly-based ids for mobile devices using machine learning classifiers," *Security Commun. Netw.*, vol. 5, no. 1, pp. 3–14, 2012.

[50] D. Damopoulos, G. Kambourakis, and S. Gritzalis, "From keyloggers to touchloggers: Take the rough with the smooth," *Comput. Security*, vol. 32, pp. 102–114, Feb. 2013.

[51] D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, and J. H. Park, "User privacy and modern mobile services: Are they on the same path?" *Pers. Ubiquitous Comput.*, vol. 17, no. 7, pp. 1437–1448, Oct. 2013.

[52] D. Damopoulos, G. Kambourakis, and G. Portokalidis, "The best of both worlds. A framework for the synergistic operation of host and cloud anomaly-based IDS for smartphones," in *Proc. 7th EuroSec Workshop Syst.*, 2014, pp. 1–6.

[53] D. Damopoulos, G. Kambourakis, S. Gritzalis, and S. O. Park, "Exposing mobile malware from the inside (or what is your mobile app really doing?)," *Peer-to-Peer Netw. Appl.*, vol. 7, no. 4, pp. 687–697, Dec. 2014.

[54] J. Dai and J. Zhou, "Multifeature-based high-resolution palmprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 5, pp. 945–957, May 2011.

[55] R. Das, "Retinal recognition—Biometric technology in practice," *Keesing J. Doc. Identity*, vol. 22, pp. 11–14, 2007.

[56] A. Das, O. K. Manyam, M. Tapaswi, and V. Taranalli, "Multilingual spoken-password based user authentication in emerging economies using cellular phone networks," in *Proc. SLT*, 2008, pp. 5–8.

[57] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 15, no. 11, pp. 1148–1161, Nov. 1993.

[58] J. Daugman, "How iris recognition works," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 21–30, Jan. 2004.

[59] G. I. Davida, Y. Frankel, and B. Matt, "On enabling secure applications through off-line biometric identification," in *Proc. IEEE Symp. Security Privacy*, 1998, pp. 148–157.

[60] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1161–1172, Dec. 2014.

[61] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, "Touch me once and I know its you! Implicit authentication based on touch screen patterns," in *Proc. CHI*, 2012, pp. 987–996.

[62] G. B. Del Pozo, C. Sanchez-Avila, A. De-Santos-Sierra, and J. Guerra-Casanova, "Speed-independent gait identification for mobile devices," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 26, no. 8, Dec. 2012, Art. ID. 1260013.

[63] R. Derakhshani, S. A. C. Schuckers, L. A. Hornak, and L. O. Gorman, "Determination of vitality from a noninvasive biomedical measurementfor use in fingerprint scanners," *Pattern Recognit.*, vol. 36, no. 2, pp. 383–396, Feb. 2003.

[64] M. O. Derawi, C. Nickely, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Proc. IIH-MSP*, 2010, pp. 306–311.

[65] M. O. Derawi, B. Yang, and C. Busch, "Fingerprint recognition with embedded cameras on mobile phones," in *Proc. MobiSec*, 2012, pp. 136–147.

[66] M. O. Derawi, "Biometric options for mobile phone authentication," *Biometric Technol. Today*, vol. 2011, no. 9, pp. 5–7, Oct. 2011.

[67] N. M. Duc and B. Q. Minh, "Your face is not your password," in *Proc. Black Hat Conference*, Las Vegas, NV, USA, 2009, pp. 1–16.

[68] N. Duta, "A survey of biometric technology based on hand shape," *Pattern Recognit.*, vol. 42, no. 11, pp. 2876–2896, Nov. 2009.

[69] B. Draffin, J. Zhu, and J. Zhang, "Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction," in *Proc. 5th Int. Conf. Mobile Comput., Appl. Serv.*, 2013, pp. 184–201.

[70] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognition-based graphical passwords on mobile devices," in *Proc. SOUPS*, 2010, pp. 1–12.

[71] N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," *Pers. Ubiquitous Comput.*, vol. 10, no. 4, pp. 255–268, May 2006.

[72] N. Eagle, A. Pentland, and D. Lazer, "Inferring friendship network structure by using mobile phone data," *Proc. Nat. Acad. Sci. USA*, vol. 106, no. 36, pp. 15 274–15 278, Sep. 2009.

[73] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[74] M. Franzgrote *et al.*, "Palmprint verification on mobile phones using accelerated competitive code," in *Proc. ICHB*, 2011, pp. 1–6.

[75] T. Feng *et al.*, "Continuous mobile authentication using touchscreen gestures," in *Proc. HST*, 2012, pp. 451–456.

[76] T. Feng, X. Zhao, B. Carbunar, and W. Shi, "Continuous mobile authentication using virtual key typing biometrics," in *Proc. TrustCom*, 2013, pp. 1547–1552.

[77] J. Fingas, "Lenovo A586 Touts Voice Unlock Through BAIDU, A∗STAR Verification Tech," Dec. 2012. [Online]. Available: http://www.engadget.com/2012/12/01/lenovo-a586-touts-voice-unlock-through-baidu-astar/

[78] R. D. Findling and R. Mayrhofer, "Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices," *Int. J. Pervasive Comput. Commun.*, vol. 9, no. 3, pp. 190–208, 2013.

[79] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song, "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 136–148, Jan. 2013.

[80] J. Frank, S. Mannor, and D. Precup, "Activity and gait recognition with time-delay embeddings," in *Proc. AAAI Conf. Artif. Intell.*, 2010, pp. 1581–1586.

[81] "Worldwide Mobile Phone Market Forecast to Grow 7.3% in 2013," Framingham, MA, USA, Sep. 2013. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS24302813

[82] FVC2006: The Fourth International Fingerprint Verification Competition. [Online]. Available: http://bias.csr.unibo.it/fvc2006/default.asp

[83] P. Gosset, "ASPeCT: Fraud detection concepts: Final report," CiteSeer, Doc Ref. AC095/VOD/W22/DS/P/18/1, pp. 1–27, 1997.

[84] A. Goode, "Bring your own finger—How mobile is bringing biometrics to consumers," *Biometric Technol. Today*, vol. 2014, no. 5, pp. 5–9, May 2014.

[85] J. Guerra-Casanova, C. Sanchez-Avila, G. Bailador, and A. de Santos Sierra, "Authentication in mobile devices through hand gesture recognition," *Int. J. Inf. Security*, vol. 11, no. 2, pp. 65–83, Apr. 2012.

[86] C. Giuffrida, K. Majdanik, M. Conti, and H. Bos, "I sensed it was you: Authenticating mobile users with sensor-enhanced keystroke dynamics," in *Proc. DIMVA*, 2014, pp. 92–111.

[87] A. Hadid, J. Y. Heikkil, O. Silven, and M. Pietikinen, "Face and eye detection for person authentication in mobile phones," in *Proc. ICDSC*, 2007, pp. 101–108.

[88] J. Hall, M. Barbeau, and E. Kranakis, "Anomaly-based intrusion detection using mobility profiles of public transportation users," in *Proc. WiMob*, 2005, pp. 17–24.

[89] Y. Han, T. Tan, Z. Sun, and Y. Hao, "Embedded palmprint recognition system on mobile devices," in *Proc. Int. Conf. Biometrics*, 2007, pp. 1184–1193.

[90] J. Han, E. Owusu, L. T. Nguyen, A. Perrig, and J. Zhang, "ACComplice: Location inference using accelerometers on smartphones," in *Proc. Int. Conf. Commun. Syst. Netw.*, 2012, pp. 1–9.

[91] T. J. Hazen, E. Weinstein, B. Heisele, A. Park, and J. Ming, "Multimodal face and speaker identification for mobile devices," in *Face Biometrics for Personal Identification*. Berlin, Germany: Springer-Verlag, 2007.

[92] J. Hu, "Mobile fingerprint template protection: Progress and open issues," in *Proc. ICIEA*, 2008, pp. 2133–2138.

[93] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[94] X. Huang, G. Lund, and A. Sapeluk, "Development of a typing behaviour recognition mechanism on android," in *Proc. TrustCom*, 2012, pp. 1342–1347.

[95] S. Hwang, S. Cho, and S. Park, "Keystroke dynamics-based authentication for mobile devices," *Comput. Security*, vol. 28, no. 1/2, pp. 85–93, Feb./Mar. 2009.

[96] Principles of Iris Biometrics. [Online]. Available: http://www.biometricnewsportal.com/iris_biometrics.asp

[97] A. K. Jain, "Biometrie recognition: Overview and recent advances," in *Proc. CIARP*, 2007, pp. 13–19.

[98] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," *Commun. ACM*, vol. 43, no. 2, pp. 91–98, Feb. 2000.

[99] I. Joe and Y. Lee, "Design of remote control system for data protection and backup in mobile devices," in *Proc. Int. Conf. Interaction Sci.*, 2011, pp. 189–193.

[100] V. John, "Motorola ATRIX 4G Review," 2011. [Online]. Available: http://www.phonearena.com/reviews/Motorola-ATRIX-4G-Review_id2665

[101] R. C. Johnson, W. J. Scheirer, and T. E. Boult, "Secure voice based authentication for mobile devices: Vaulted voice verification," in *Proc. SPIE*, 2013, pp. 87120P-1–87120P-13.

[102] L. A. Jones, A. I. Anton, and J. B. Earp, "Towards understanding user perceptions of authentication technologies," in *Proc. ACM Workshop Privacy Electron. Soc.*, 2007, pp. 91–98.

[103] K. H. Kamer, A. Yuksel, A. Jahnbekam, M. Roshan-del, and D. Skirpo, "MagiSign: User identification/authentication based on 3D around device magnetic signatures," in *Proc. Ubicomm*, 2010, pp. 31–34.

[104] J.-S. Kang, "Mobile iris recognition systems: An emerging biometric technology," *Procedia Comput. Sci.*, vol. 1, no. 1, pp. 475–484, May 2010.

[105] P. Kang and S. Cho, "Keystroke dynamics-based user authentication using long and free text strings from various input devices," *Inf. Sci.*, 2014, DOI: 10.1016/j.ins.2014.08.070, to be published.

[106] A. K. Karlson, A. B. Brush, and S. Schechter, "Can I borrow your phone?: Understanding concerns when sharing mobile phones," in *Proc. CHI*, 2009, pp. 1647–1650.

[107] S. Karatzouni and N. Clarke, "Keystroke analysis for thumb-based keyboards on mobile devices," in *Proc. IFIP Int. Inf. SEC*, 2007, pp. 253–263.

[108] S. Karatzouni, N. L. Clarke, and S. M. Furnell, "Document utilising biometrics for transparent user authentication on mobile devices," in *Proc. ITA*, 2007, pp. 549–557.

[109] H. Ketabdar, P. Moghadam, B. Naderi, and M. Roshandel, "Magnetic signatures in air for mobile devices," in *Proc. MobileHCI*, 2012, pp. 185–188.

[110] H. Khan, A. Atwater, and U. Hengartner, "Itus: An implicit authentication framework for android," in *Proc. MobiCom*, 2014, pp. 507–518.

[111] S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," *Pattern Recognit.*, vol. 48, no. 2, pp. 458–472, Feb. 2015.

[112] P. Khaw, *Iris Recognition Technology for Improved Authentication*. Singapore: SANS Institute, 2002.

[113] E. Khoury, L. El Shafey, C. McCool, M. Gunther, and S. Marcel, "Bi-modal biometric authentication on mobile phones in challenging conditions," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1147–1160, Dec. 2013.

[114] D.-J. Kim, K.-W. Chung, and K.-S. Hong, "Person authentication using face, teeth and voice modalities for mobile device security," *IEEE Trans. Consum. Electron.*, vol. 56, no. 4, pp. 2678–2685, Nov. 2010.

[115] D.-J. Kim and K.-S. Hong, "Multimodal biometric authentication using teeth image and voice in mobile environment," *IEEE Trans. Consum. Electron.*, vol. 54, no. 4, pp. 1790–1797, Nov. 2008.

[116] D.-J. Kim, J.-H. Shin, and K.-S. Hong, "Teeth recognition based on multiple attempts in mobile device," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 283–292, May 2010.

[117] T. Kinnunen *et al.*, "Vulnerability of speaker verification systems against voice conversion spoofing attacks: The case of telephone speech," in *Proc. IEEE ICASSP*, 2012, pp. 4401–4404.

[118] K. Kollreider, H. Fronthaler, and J. Bigun, "Verifying liveness by multiple experts in face biometrics," in *Proc. IEEE Comput. Vis. Pattern Recog. Workshop Biometrics*, 2008, pp. 1–6.

[119] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244, Feb. 2009.

[120] A. Kong, D. Zhang, and M. Kamel, "A survey of palmprint recognition," *Pattern Recognit.*, vol. 42, no. 7, pp. 1408–1418, Jul. 2009.

[121] C. Köse and C. İkibaş, "A personal identification system using retinal vasculature in retinal fundus images," *Expert Syst. Appl.*, vol. 38, no. 11, pp. 13670–13681, Oct. 2011.

[122] J. Kraunelis, Y. Chen, Z. Ling, X. Fu, and W. Zhao, "On malware leveraging the android accessibility framework," in *Proc. MobiQuitous*, 2014, pp. 512–523.

[123] D. F. Kune and Y. Kim, "Timing attacks on PIN input devices," in *Proc. ACM Conf. CCS*, 2010, pp. 678–680.

[124] M. Kunz, K. Kasper, H. Reininger, M. Mobius, and J. Ohms, "Continuous speaker verification in realtime," in *Proc. Int. Conf. Biometrics Special Interest Group*, 2011, pp. 79–87.

[125] M. La Polla, F. Martinelli, and D. Sgandurra, "A survey on security for mobile devices," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 446–471, 2013.

[126] N. D. Lane *et al.*, "A survey of mobile phone sensing," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 140–150, Sep. 2010.

[127] G. Lawton, "Is it finally time to worry about mobile malware?" *Computer*, vol. 41, no. 5, pp. 12–14, May 2008.

[128] C. Lee, J. Y. Choi, K. A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutia information," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 37, no. 4, pp. 980–992, Aug. 2007.

[129] D. Lee, "The State of the Touch-Screen Panel Market in 2011," 2011. [Online]. Available: http://www.walkermobile.com/March_2011_ID_State_of_the_Touch_Screen_Market.pdf

[130] L. Li, X. Zhao, and G. Xue, "Unobservable re-authentication for smartphones," in *Proc. NDSS*, 2013, pp. 1–16.

[131] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Behaviour profiling for transparent authentication for mobile devices," in *Proc. Eur. Conf. Inf. Warfare Security*, 2011, pp. 307–314.

[132] F. Li, N. Clarke, M. Papadaki, and P. Dowland, "Active authentication for mobile devices utilising behaviour profiling," *Int. J. Inf. Security*, vol. 13, no. 3, pp. 229–244, Jun. 2014.

[133] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," in *Proc. ASIACCS*, 2014, pp. 413–424.

[134] Z. Liu and S. Song, "An embedded real-time finger-vein recognition system for mobile devices," *IEEE Trans. Consum. Electron.*, vol. 58, no. 2, pp. 522–527, May 2012.

[135] L. Long, "Biometrics: The future of mobile phones," in *Proc. Interactive Multimedia Conf.*, 2014, pp. 1–5.

[136] D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 3, pp. 402–412, Mar. 2002.

[137] E. Maiorana, P. Campisi, N. Gonzalez-Carballo, and A. Neri, "Keystroke dynamics authentication for mobile phones," in *Proc. ACM SAC*, 2011, pp. 21–26.

[138] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S.-M. Makela, and H. Ailisto, "Identifying users of portable devices from gait pattern with accelerometers," in *Proc. IEEE ICASSP*, 2005, pp. 973–976.

[139] P. Marquardt, A. Verma, H. Carter, and P. Traynor, "(sp)iphone: Decoding vibrations from nearby keyboards using mobile phone accelerometers," in *Proc. CCS*, 2011, pp. 551–562.

[140] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "Towards mobile authentication using dynamic signature verification: Useful features and performance evaluation," in *Proc. ICPR*, 2008, pp. 1–5.

[141] R. A. Maxion and K. S. Killourhy, "Keystroke biometrics with number-pad input," in *Proc. DSN*, 2010, pp. 201–210.

[142] V. Matyas, Jr. and Z. Riha, "Toward reliable user authentication through biometrics," *IEEE Security Privacy*, vol. 1, no. 3, pp. 45–49, May/Jun. 2003.

[143] Y. Meng, D. S. Wong, R. Schlegel, and L. F. Kwok, "Touch gestures based biometric authentication scheme for touchscreen mobile phones," in *Proc. 8th Int. Conf. INSCRYPT*, 2012, pp. 331–350.

[144] Y. Meng, D. S. Wong, and L. F. Kwok, "Design of touch dynamics based user authentication with an adaptive mechanism on mobile phones," in *Proc. Annu. ACM SAC*, 2014, pp. 1680–1687.

[145] W. Meng, D. S. Wong, and L. F. Kwok, "The effect of adaptive mechanism on behavioural biometric based mobile phone authentication," *Inf. Manage. Comput. Security*, vol. 22, no. 2, pp. 155–166, 2014.

[146] T. C. Meng, P. Gupta, and D. Gao, "I can be you: Questioning the use of keystroke dynamics as biometrics," in *Proc. NDSS*, 2013, pp. 1–16.

[147] E. Miluzzo *et al.*, "Darwin phones: The evolution of sensing and inference on mobile phones," in *Proc. MobiSys*, 2010, pp. 5–20.

[148] E. Miluzzo, A. Varshavsky, S. Balakrishnan, and R. R. Choudhury, "Tapprints: Your finger taps have fingerprints," in *Proc. MobiSys*, 2012, pp. 323–336.

[149] N. F. Moco, I. S. Tecnico, I. De Telecomunicacoes, and P. L. Correia, "Smartphone-based palmprint recognition system," in *Proc. ICT*, 2014, pp. 457–461.

[150] A. C. Morris *et al.*, "Multimodal person authentication on a smartphone under realistic conditions," in *Proc. SPIE*, 2006, Art. ID. 62500D.

[151] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in *Proc. 6th ACM Conf. CCS*, 1999, pp. 73–82.

[152] M. Muaaz and R. Mayrhofer, "An analysis of different approaches to gait recognition using cell phone based accelerometers," in *Proc. MoMM*, 2013, p. 293.

[153] L. Myers, "*An Exploration of Voice Biometrics.*," Singapore: SANS Institute, 2004.

[154] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Proc. IIH-MSP*, 2012, pp. 16–20.

[155] S. Narayanaswamy, J. Hu, and R. Kashi, "User interface for a PCS smart phone," in *Proc. IEEE Int. Conf. Multimedia Comput. Syst.*, 1999, pp. 777–781.

[156] C. Nickel, C. Busch, S. Rangarajan, and M. Mobius, "Using hidden Markov models for accelerometer-based biometric gait recognition," in *Proc. CSPA*, 2011, pp. 58–63.

[157] I. Oakley and A. Bianchi, "Multi-touch passwords for mobile device access," in *Proc. UbiComp*, 2012, pp. 611–612.

[158] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "ACCessory: password inference using accelerometers on smartphones," in *Proc. HotMobile*, 2012, pp. 1–6.

[159] D. J. Ohana, L. Phillips, and L. Chen, "Preventing cell phone intrusion and theft using biometrics," in *Proc. IEEE Security Privacy Workshops*, 2013, pp. 173–180.

[160] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Proc. IEEE 11th ICCV*, 2007, pp. 1–8.

[161] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eye-blink and scene context," *J. Telecommun. Syst.*, vol. 47, no. 3/4, pp. 215–225, Aug. 2009.

[162] D. Papamartzivanos, D. Damopoulos, and G. Kambourakis, "A cloud-based architecture to crowdsource mobile app privacy leaks," in *Proc. 18th PCI*, 2014, pp. 1–6.

[163] K. R. Park, H.-A. Park, B. J. Kang, E. C. Lee, and D. S. Jeong, "A study on iris localization and recognition on mobile phones," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. 1, p. 281 943, Oct. 2008.

[164] Y. S. Park, S. H. Han, J. Park, and Y. Cho, "Touch key design for target selection on a mobile phone," in *Proc. MobileHCI*, 2008, pp. 423–426.

[165] A. Pabbaraju and S. Puchakayala, "Face recognition in mobile devices," Univ. Michigan, Ann Arbor, MI, USA, Final Rep., 2010.

[166] S. Peng, S. Yu, and A. Yang, "Smartphone malware and its propagation modeling: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 925–941, 2014.

[167] K. A. Rahman, K. S. Balagani, and V. V. Phoha, "Making impostor pass rates meaningless: A case of snoop-forge-replay attack on continuous cyber-behavioural verification with keystrokes," in *Proc. CVPRW*, 2011, pp. 31–38.

[168] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[169] N. Ratha, S. Chikkerur, J. H. Connel, and R. M. Bolle, "Generating cancellable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[170] H. Ravi and S. K. Sivanath, "A novel method for touch-less finger print authentication," in *Proc. IEEE Int. Conf. Technol. HST*, 2013, pp. 147–153.

[171] O. Riva, C. Qin, K. Strauss, and D. Lymberopoulos, "Progressive authentication: Deciding when to authenticate on mobile phones," in *Proc. 21st USENIX Security Symp.*, 2012, pp. 1–16.

[172] R. N. Rodrigues *et al.*, "Biometric access control through numerical keyboards based on keystroke dynamics," in *Proc. ICB Adv.*, 2005, pp. 640–646.

[173] M. Rogowski, K. Saeed, M. Rybnik, M. Tabedzki, and M. Adamski, "User authentication for mobile devices," in *Proc. CISIM*, 2013, pp. 47–58.

[174] J. Rokita, A. Krzyzak, and C. Y. Suen, "Cell phones personal authentication systems using multimodal biometrics," in *Proc. ICIAR*, 2008, pp. 1013–1022.

[175] V. Ruiz-Albacete *et al.*, "Direct attacks using fake images in iris verification," in *Biometrics and Identity Management*. Berlin, Germany: Springer-Verlag, 2008, pp. 181–190.

[176] H. Saevanee and P. Bhattarakosol, "Authenticating user using keystroke dynamics and finger pressure," in *Proc. 6th IEEE Consum. Commun. Netw. Conf.*, 2009, pp. 1078–1079.

[177] H. Saevanee, N. Clarke, and S. Furnell, "SMS linguistic profiling authentication on mobile device," in *Proc. 5th Int. Conf. NSS*, 2011, pp. 224–228.

[178] H. Saevanee, N. L. Clarke, and S. M. Furnell, "Multi-modal behavioural biometric authentication for mobile devices," in *Proc. IFIP Inf. SEC Privacy Conf.*, 2012, pp. 465–474.

[179] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon, "Biometric-rich gestures: A novel approach to authentication on multitouch devices," in *Proc. CHI*, 2012, pp. 977–986.

[180] N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp. 933–947, Jun. 2014.

[181] N. Sae-Bae, N. Memon, K. Isbister, and K. Ahmed, "Multitouch gesture-based authentication," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 568–582, Apr. 2014.

[182] J. Pramis, EyeVerify Developing an Eye-Scanning Unlock Tool for your Phone, Mar. 2013. [Online]. Available: http://www.digitaltrends.com/mobile/eyeverify-retinal-scan-lock/

[183] *SAGEM Points a Finger at GSM*, SAGEM, Paris, France, Jan. 24, 2000, Press Release.

[184] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "SmudgeSafe: Geometric image transformations for smudge-resistant user authentication," in *Proc. Ubicomp*, 2014, pp. 775–786.

[185] R. Schlegel *et al.*, "Soundcomber: A stealthy and context-aware sound trojan for smartphones," in *Proc. NDSS*, 2011, pp. 17–33.

[186] N. A. Schmid, M. V. Ketkar, H. Singh, and B. Cukic, "Performance analysis of iris-based identification system at the matching score level," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 154–168, Jun. 2006.

[187] A.-D. Schmidt, F. Peters, F. Lamour, and S. Albayrak, "Monitoring smartphones for anomaly detection," in *Proc. MOBILWARE*, 2008, pp. 40:1–40:7.

[188] A.-D. Schmidt *et al.*, "Monitoring smartphones for anomaly detection," *Mobile Netw. Appl.*, vol. 14, no. 1, pp. 92–106, Feb. 2009.

[189] A.-D. Schmidt *et al.*, "Smartphone malware evolution revisited: Android next target?" in *Proc. MALWARE*, 2009, pp. 1–7.

[190] A. Serwadda, V. V. Phoha, and A. Kiremire, "Using global knowledge of users' typing traits to attack keystroke biometrics templates," in *Proc. MM Sec*, 2011, pp. 51–60.

[191] A. Shabtai *et al.*, "Google android: A comprehensive security assessment," *IEEE Security Privacy*, vol. 8, no. 2, pp. 35–44, Mar./Apr. 2010.

[192] M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: You can see it but you can not do it," in *Proc. MobiCom*, 2013, pp. 39–50.

[193] A. Shabtai, U. Kanonov, and Y. Elovici, "Intrusion detection for mobile devices using the knowledge-based, temporal abstraction method," *J. Syst. Softw.*, vol. 83, no. 8, pp. 1524–1537, Aug. 2010.

[194] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *J. Verbal Learn. Verbal Behav.*, vol. 6, no. 1, pp. 156–163, Feb. 1967.

[195] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong, "Senguard: Passive user identification on smartphones using multiple sensors," in *Proc. 7th Int. Conf. WiMob Comput., Netw. Commun.*, 2011, pp. 141–148.

[196] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," in *Proc. ISC*, 2011, pp. 99–113.

[197] S. Shirazi, A. P. Moghadam, H. Ketabdar, and A. Schmidt, "Assessing the vulnerability of magnetic gestural authentication to video-based shoulder surfing attacks," in *Proc. CHI*, 2012, pp. 2045–2048.

[198] K. A. Sidek, V. Mai, and I. Khalil, "Data mining in mobile ECG based biometric identification," *J. Netw. Comput. Appl.*, vol. 44, pp. 83–91, Sep. 2014.

[199] S. Sin, R. Zhou, D. Li, T. Isshiki, and H. Kunieda, "Narrow fingerprint sensor verification with template updating technique," *IEICE Trans. Fundam. Electron.*, vol. 95, no. 1, pp. 346–353, Jan. 2012.

[200] D. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on SSH," in *Proc. 10th Conf. USENIX Security Symp.*, 2001, pp. 25:1–25:17.

[201] *Password Unseated by "123456" on SplashData's Annual Worst Passwords List*, SplashData, Inc., Los Gatos, CA, USA, 2013.

[202] A. Srinivasan and J. Wu, "SafeCode: Safeguarding security and privacy of user data on stolen iOS devices," in *Cyberspace Safety and Security*. Berlin, Germany: Springer-Verlag, 2012, pp. 11–20.

[203] D. Stefan, X. Shu, and D. Yao, "Robustness of keystroke-dynamics based biometrics against synthetic forgeries," *Comput. Security*, vol. 31, no. 1, pp. 109–121, Feb. 2012.

[204] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 961–987, 2014.

[205] M. Sujithra and G. Padmavathi, "Next generation biometric security system: An approach for mobile device security," in *Proc. CCSEIT*, 2012, pp. 371–381.

[206] B. Suhm, B. Myers, and A. Waibel, "Multimodal error correction for speech user," *ACM Trans. Comput.-Human Interact.*, vol. 8, no. 1, pp. 60–98, Mar. 2001.

[207] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Touchin: Sightless two factor authentication on multitouch mobile devices," in *Proc. CoRR*, 2014, pp. 1–14.

[208] Q. Tao and R. Veldhuis, "Biometric authentication system on mobile personal devices," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 763–773, Apr. 2010.

[209] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proc. SOUPS*, 2006, pp. 56–66.

[210] C.-J. Tasia, T.-Y. Chang, P.-C. Cheng, and J.-H. Lin, "Two novel biometric features in keystroke dynamics authentication systems for touch screen devices," *Security Commun. Netw.*, vol. 7, no. 4, pp. 750–758, Apr. 2014.

[211] R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, "PlaceRaider: Virtual theft in physical spaces with smartphones," in *Proc. NDSS*, San Diego, CA, USA, 2013, pp. 1–15.

[212] H. M. Thang, V. Q. Viet, N. Dinh Thuc, and D. Choi, "Gait identification using accelerometer on mobile phone," in *Proc. ICCAIS*, 2012, pp. 344–348.

[213] J. Trader, "Vodaphone in UK Using M2SYS Hybrid Biometric Platform & Palm Vein Biometrics at Summer Festivals,", Jun. 2012. [Online]. Available: http://blog.m2sys.com/biometric-hardware/vodaphone-in-uk-using-m2sys-hybrid-biometric-platform-palm-vein-biometrics-at-summer-festivals/

[214] S. Trewin *et al.*, "Biometric authentication on a mobile device: A study of user effort, error and task disruption," in *Proc. 28th ACSAC*, 2012, pp. 159–168.

[215] H. Victor, "Apple iPhone 5S: 7 New Features of the Seventh Generation iPhone," Sep. 2013. [Online]. Available: http://www.phonearena.com/news/Apple-iPhone-5S-7-new-features-of-the-seventh-generation-iPhone_id46538

[216] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," in *Proc. 18th Conf. USENIX Security Symp.*, 2009, pp. 1–16.

[217] R. Wallace, M. McLaren, C. McCool, and S. Marcel, "Cross-pollination of normalisation techniques from speaker to face authentication using Gaussian mixture models," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 553–562, Apr. 2012.

[218] M. Warman, Say Goodbye to the Pin: Voice Recognition Takes Over at Barclays Wealth, May 2013. [Online]. Available: http://www.telegraph.co.uk/technology/news/10044493/Say-goodbye-to-the-pin-voice-recognition-takes-over-at-Barclays-Wealth.html

[219] T. Werthmann, R. Hund, L. Davi, A.-R. Sadeghi, and T. Holz, "PSiOS: Bring your own privacy & security to iOS devices," in *Proc. ASIACCS*, 2013, pp. 13–24.

[220] T. J. Wixted, "The psychology and neuroscience of forgetting," *Annu. Rev. Psychol.*, vol. 55, pp. 235–269, 2004.

[221] M. Wolf, "Behavioral biometric identification on mobile devices," in *Proc. AC/HCII*, 2013, pp. 783–791.

[222] K. Xi, J. Hu, and F. Han, "Mobile device access control: An improved correlation based face authentication scheme and its Java ME application," *Concurr. Comput. Pract. Exp.*, vol. 24, no. 10, pp. 1066–1085, Jul. 2012.

[223] K. Xi and J. Hu, "Biometric mobile template protection: A composite feature based fingerprint fuzzy vault," in *Proc. IEEE ICC*, 2009, pp. 829–833.

[224] L. Xing, X. Pan, R. Wang, K. Yuan, and X. Wang, "Upgrading your android, elevating my malware: Privilege escalation through mobile OS updating," in *Proc. IEEE Symp. Security Privacy*, 2014, pp. 393–408.

[225] N. Xu *et al.*, "Stealthy video capturer: A new video-based spyware in 3G smartphones," in *Proc. WiSec*, 2009, pp. 69–78.

[226] Z. Xu, K. Bai, and S. Zhu, "Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors," in *Proc. WiSec*, 2012, pp. 1–12.

[227] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proc. SOUPS*, 2014, pp. 187–198.

[228] Q. Yan, J. Han, Y. Li, J. Zhou, and R. H. Deng, "Designing leakage-resilient password entry on touchscreen mobile devices," in *Proc. ASIACCS*, 2013, pp. 37–48.

[229] J. Yang, "Trends and Forecast for 2013 Touch Panel Market," Dec. 2012. [Online]. http://www.digitimes.com/news/a20121228RS401.html?mod=0&chid=2T

[230] R. V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: A survey and classification," *Int. J. Biometrics*, vol. 1, no. 1, pp. 81–113, Jun. 2008.

[231] B. Yirka, "Japanese Partnership Results in Palm Recognition Security for Smartphones," 2012. [Online]. Available: http://phys.org/news/2012-09-japanese-partnership-results-palm-recognition.html

[232] X. Yu *et al.*, "Remotely wiping sensitive data on stolen smartphones," in *Proc. ASIACCS*, 2014, pp. 537–542.

[233] S. Zahid, M. Shahzad, S. A. Khayam, and M. Farooq, "Keystroke-based user identification on Smart phones," in *Proc. RAID*, 2009, pp. 224–243.

[234] X. Zhang and Y. Gao, "Face recognition across pose: A review," *Pattern Recognit.*, vol. 42, no. 11, pp. 2876–2896, Nov. 2009.

[235] D. Zhang, W. Zuo, and F. Yue, "A comparative study of palmprint recognition algorithms," *ACM Comput. Surveys*, vol. 44, no. 1, pp. 1–37, Jan. 2012.

[236] Y. Zhang *et al.*, "Fingerprint attack against touch-enabled devices," in *Proc. SPSM*, 2012, pp. 57–68.

[237] X. Zhao, T. Feng, and W. Shi, "Continuous mobile authentication using a novel graphic touch gesture feature," in *Proc. 6th Int. Conf. Biometrics—Theory, Appl. Syst.*, 2013, pp. 1–6.

[238] M. Zhao, T. Zhang, F. Ge, and Z. Yuan, "RobotDroid: A lightweight malware detection framework on smartphones," *J. Netw.*, vol. 7, no. 4, pp. 715–722, Apr. 2012.

[239] M. Zhao, T. Zhang, J. Wang, and Z. Yuan, "A smartphone malware detection framework based on artificial immunology," *J. Netw.*, vol. 8, no. 2, pp. 469–476, Feb. 2013.

[240] L. Zhuang, F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," *ACM Trans. Inf. Syst. Security*, vol. 13, no. 1, pp. 3:1–3:26, Oct. 2009.

[241] N. Zheng, A. Paloski, and H. Wang, "An efficient user verification system via mouse movements," in *Proc. ACM Conf. CCS*, 2011, pp. 139–150.

[242] Y. Zhou and X. Jiang, "Dissecting android malware: Characterization and evolution," in *Proc. IEEE Symp. Security Privacy*, 2012, pp. 95–109.

[243] J. Zhu, P. Wu, X. Wang, and J. Zhang, "SenSec: Mobile security through passive sensing," in *Proc. 13th ICNC*, 2013, pp. 1128–1133.

Weizhi Meng received the Bachelor's degree in computer science (information security) from Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and the Ph.D. degree in computer science from the City University of Hong Kong, Kowloon, Hong Kong, in 2013. He was previously known as Yuxin Meng and is currently a Research Scientist with the Infocomm Security Department, Institute for Infocomm Research, Singapore. Prior to this, he was a Senior Research Associate with the Department of Computer Science, City University of Hong Kong. His research interests include information security including intrusion detection, mobile security, cloud computing, and intelligent security applications.

Duncan S. Wong received the B.Eng. degree in electrical and electronic engineering from the University of Hong Kong, Pokfulam, Hong Kong, in 1994; the M.Phil. degree in information engineering from the Chinese University of Hong Kong, Shatin, Hong Kong, in 1998; and the Ph.D. degree in computer science from Northeastern University, Boston, MA, USA, in 2002. He is currently an Associate Professor with the Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong. His primary research interest is cryptography, including network security, wireless security, database security, and security in cloud computing.

Steven Furnell received a Ph.D. degree in information system security from the University of Plymouth in 1995, and now is the Head of the Centre for Security, Communications and Network Research at Plymouth University, U.K., and an Adjunct Professor with Edith Cowan University, Perth, Australia. Prof. Furnell is the author of over 250 papers in refereed international journals and conference proceedings, as well as books including Cybercrime: Vandalising the Information Society (2001) and Computer Insecurity: Risking the System (2005). His interests include security management and culture, computer crime, user authentication, and security usability. Further details can be found at www.plymouth.ac.uk/cscan, with a variety of security podcasts also available via www.cscan.org/podcasts.

Jianying Zhou received the Ph.D. degree in information security from the University of London, London, U.K., in 1997. He is a Senior Scientist with the Institute for Infocomm Research and the Head of the Infocomm Security Department. His research interests include computer and network security and mobile and wireless security. He is a Cofounder and a Steering Committee Member of the International Conference on Applied Cryptography and Network Security (ACNS).