Adoption of biometrics in mobile devices

Esmeralda Kadëna, Lourdes Ruiz

Óbuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary

kadena.esmeralda@phd.uni-obuda.hu, lourdes.ruiz@ bgk.uni-obuda.hu

Abstract: Mobile phones are quickly becoming the most popular and widely used form of communication. Mobile phones are commonly used for web-surfing, products and services payments as well as storing of sensitive data and information. The increasing number of users and security risks imply a need for an improved protection of users' personal data, such as health information, personal identifiers, financial data and so on. One useful tool to address this need is biometric authentication. In this work we will analyze the adoption of biometrics in mobile devices by describing the past and present applications and how the future is shaping regarding this technology.

1. Introduction

Over the last years, information access from mobile devices has become mainstream both in business and personal environments. The world is becoming more and more connected and every mobile user wants to be sure about personal data security. For many years, the only secured way of authentication was the password. During the last years and we have seen a significant rise in the use of biometrics to replace passwords because the technology has proven to be much more convenient and less time-consuming than passwords. There are several concerns related to mobile phone security such as information loss, phone theft and mobile services usage that biometric systems help to address them. So as a result we have a winning combination of mobile devices and biometrics in the mass market which allows the technology to become much more widely accepted.

Mobile biometrics refers to the deployment of biometric authentication methods on mobile devices such as smartphones and tablets. The rich set of input sensors on mobile devices, including cameras, microphones, and touchscreens enable sophisticated multimedia interactions [1]. A biometric system can measure

physical or behavioral characteristics such as fingerprint, palmprint, face, iris, retina, ear, voice, signature, gait, hand vein, odor, or the DNA[8] information of an individual to determine or verify his identity [2]. It consists on the following units:

- A sensor: represents the interface between the user and the machine;
- A processing: where the acquired biometric is sampled, segmented and features are being extracted. It also includes quality assurance to determine if the quality of the biometric is good enough to be used further in the process. If the quality of the acquired biometric is poor, the user may be asked to present the biometric again;
- A database: where all the enrolled biometric templates are being stored and where the templates are being retrieved from in the authentication process;
- A matching unit that compares the newly acquired biometric template with the templates stored in the database and based on decision rules determines either if the presented biometric is a genuine/impostor or if the user is identified or not.

2. Implementation of Biometrics

There are two modes that biometric systems can be integrated in mobile devices:

a. *Network mode (as an on-line device):* device collects data and passes it online via Internet to a remote location where it is processed and compared. This proves useful for remote transactions when the identity of the caller has to be proven. As an example when a user calls his/her bank to make a transaction, he/she is going to introduce herself and in order to verify identity is asked to recite a pass-phrase. The voice recording is then processed and compared to the sample that was collected when the user enrolled in the system. Other biometrics traits that smartphones have the capabilities to collect and transfer them to a remote location are face, fingerprint, signature, gait, gesture or keystroke.

b. *Standalone mode (off-line)*: to protect unauthorized use of the mobile phone, the entire biometric system resides on the mobile phone and it serves the purpose of preventing unauthorized access to mobile phone functions and data. Ideal for use with large databases. It quickly captures the fingerprint image and sends the encrypted template to the biometric authentication server. Implementations of biometric systems on mobile

8 DNA: Deoxyribonucleic acid, which contains the genetic information necessary for the development and functioning of living organisms.

phones include fingerprint recognition, voice recognition, face recognition, signature recognition, gait recognition, gesture recognition and keystroke dynamics.

2.1. Voice recognition

Voice recognition appeared in 1950 and was later implemented in PCs without success. Its functioning relies on performing statistical models of the spoken language. The introduction of this technology in mobile phones was very rudimentary due to the lack of phone memory capacity. The technology started performing basic functions such as: dialing digit by digit, recognizing names, and hands-free calling. Memory, processing capabilities and network speed increased rapidly throughout time, offering better recognition abilities to mobile phones. In 2005 Samsung launched the phone model SCH-p-207, which has speech dictation and voice dialing [3]. Google Now and Siri are voice powered assistants that use natural language processing, developed by Google and Apple respectively. Google Now was launched on 2012 as a mobile application, while Siri was presented on 2011 as a built-in feature in iPhone 4s. These two intelligent assistants can perform infinite tasks within the smartphone.

2.2. Face and Iris recognition

In 2005, ClassifEye and Omron developed the first face recognition biometric as security system in camera-enabled mobile phones. This technology didn't require any additional hardware because cameras already existed in most of the phones [4]. Android's face unlock was introduced in 2011. This face recognition system presented various flaws including security issues. It needed to be used in illuminated areas in order to unlock the phone [5]. Moreover, a printed or digital photo of the user's face was sufficient to gain access to the phone.

Samsung also offers in their phones Galaxy Note7, Galaxy S8 and Note 8 an iris scanning technology that functions by identifying the unique eye iris pattern. The phone possesses an infrared diode that illuminates the eyes regarding lighting conditions. An infrared narrow focus camera takes de iris pattern information, which is stored and processed in the phone [6].

2.3. Fingerprint recognition

It is the most popular form of biometric identification. Toshiba G500 and G900 in 2007 were the first mobile phones with a fingerprint scanner [7]. But Apple was the first company that launched fingerprint recognition in smartphones by investing $356 million to acquire AuthenTec, a company focused on fingerprint reading

and identification management software [8] [9]. The iPhone 5S was introduced on September 10, 2013 [10]. It was the first phone on a major US carrier since the Atrix to feature the technology [11]. In that time was predicted that a fingerprint sensor in the iPhone 5S would help mobile commerce and boost adoption in the corporate environment [12].

During 2014 and 2015 other smartphone companies included fingerprint scanning in their high-end phones during 2014 and 2015 [13]. Starting with the Samsung Galaxy S, Android 6.0 (Android Marshmallow, released October 2015), in which the fingerprint scanner support was integrated into the operating system like Touch ID in iOS, then with HTC and Motorola. In September 2014 came with iPhone 6 and 6 Plus an expansion of Touch ID. The new feature was from being used to unlock the device and authenticating App Store purchases to also authenticating Apple Pay.

Use and implementation of biometrics in mobile phones is further enhanced by combining the technology with existing mobile phone security arrangements. For instance, a mobile phone user may have to authorize his mobile banking transactions through biometric recognition as well as using passwords and SMS codes. This is indeed a more and more elaborate security arrangement for the people who are highly dependent upon mobile phones for a variety of purposes that demand high-end security.

Previous research on using biometrics in mobile phones had already been introduced before. In 2005, Cho et al. [14] proposed a pupil and iris localization algorithm, which is apt for mobile phone platform based on detecting dark pupil and corneal specular reflection by changing brightness and contrast value. A year after, Okumura et al. [15] proposed a system where a subject could authenticate himself/herself by grasping and shaking the phone. In this study a normal accelerometer with the size of a mobile phone was used. In 2007, Hadid et al. [16] described and analyzed a face authentication system for person authentication by attaching the camera of the phone in front of the subjects face. At the same year a prototype was designed on how microphone in a mobile phone and its camera could perform voice and fingerprint recognition [17]. This work was continued by Wang et al [18] in 2009, who fused these two biometric features together retrieving acceptable results. In 2011, Conti et al. [19] proposed a biometric measure to authenticate the user of a smartphone i.e. the movement the user performs when answering a phone call.

3. Today and tomorrow

According to the International Telecommunication Union, there are more than 7 billion mobile subscriptions in the world [20]. This number is getting closer to the total world population. As the consumers are growing, biometric technology as an authentication system is wide spreading in smartphones.

The biometric characteristics commonly used in smartphones nowadays are: fingerprint, facial, voice recognition and iris scanning.

Fingerprint

Fingerprint biometrics has the biggest market share due to the increasing adoption of fingerprint reader technology by various smartphone manufacturers and according to Statistics MRC is expected to reach $52.61billion by 2022.

Apple pioneered the fingerprint feature in mobile phones which leaded to other companies to follow the same path and introduce this technology in the design of their products. Fingerprint authentication is the most popular biometric characteristic used in mobile phones nowadays. This technology is becoming very affordable for consumers, as an example T-Mobile's Revvl phone possesses a fingerprint sensor. Its price is very convenient ($125), which will increase the propagation of this biometric technology [21].

Face Recognition

Face recognition is nowadays used in smartphones such as Galaxy 8 or Note 8. The latest face recognition introduction in mobile phones was presented in 2017 by Apple in its newest model: iPhone X which possess a face recognition system called Face ID. It uses a true depth camera setup which projects more than 30000 invisible dots and scans the face in 3D. The fact that the device is creating a 3D map of the face prevents forfeiting such as face printouts. Apple assures that the face authentication system will work in poor illumination conditions, when the person is not paying attention, if there are changes in the face such as facial hair or the individual is using accessories such as hats or sunglasses [22]. Even though these asseverations, the system failed to work on the demonstration stage in September 2017.

Apple shifted its biometric identifier from fingerprint to face recognition. As it happened with the implementation of Touch ID, it is expected that other phone manufacturers will follow the path into face recognition systems.

Voice Recognition

This technology has improved, by using big data and deep learning on its neural networks in order to obtain faster and accurate results. Nowadays, voice commands in smart phones can perform infinite tasks such as the basics: making a

call, send a text or an email, set an alarm or more advanced such as set a reminder based on place or time, schedule a calendar entry, launch an app, get scores and statistics in almost any sports, play music, identify a song that is playing, get movie show times, post to social media, check the weather anywhere, search the web and answer any question. Moreover, according to a study done by Stanford, speech recognition software is faster and more accurate composing messages than humans when typing on a mobile phone. The results didn't change using different languages, for English the software was three times faster than typing and for mandarin it was 2.8 times faster [23]. Hence, this is a powerful technology that will be used for long time as an interaction between humans and machines.

As biometric technology is gaining acceptance by the public, in the near future, it will be a common practice to use biometric identifiers for authenticating an individual's identity using mobile phone as a tool. Its main usage will be for patient identification in healthcare, time attendance at the workplace and banking.

According to a study made by Gartner Inc, mobile users resist to use long and difficult passwords in their phones or tablets [24]. A market research done by Acuity, predicts that 100 percent of smartphones will have built-in biometric sensors by 2018 [25] in order to provide data security and enhance user experience. Moreover, it is expected that all smartphones in the future will integrate more than one biometric sensor. Hence the customer can decide what authentication method to use.

Regarding fingerprint technology, Apple and Samsung are developing fingerprint scanners that will be integrated in the screen replacing the button biometric built-in sensors manufactured in older phones. Additionally fingerprint sensors will be embedded in more than half of all smartphones by 2019 [26].

As for voice recognition, it is expected that more mobile applications use this technology, where voice commands are used in conjunction with a graphic interface.

Smartphones are becoming ubiquitous in everyone's life. They contain vital information regarding every aspect of a person's life. Consequently, in terms of security, privacy issues regarding the storage and usage of biometric identifiers is a major concern. According to phone manufacturers, the biometric characteristic is just stored in the phone and will not be uploaded to any remote server.

Conclusions

Using biometrics in mobile phones has expanded rapidly. In this work we presented the adoption of these systems by introducing the changes over the last years. Smartphones possess different biometric authentication systems and the technology is indeed surpassing traditional authentication methods such as passwords or pin codes. This has happened mostly for two reasons, security and

convenience. But with comfort and convenience also come some security risks. Mobile phones are acquiring this technology, but it is important to use it in conjunction with a password or pin code in a multifactor security system in order to enhance safety.

These systems are not infallible and are prone to be hacked. It is fundamental for manufacturing companies to develop devices that prevent these security risks and protect information stored in the mobile phones. Security concerns regarding biometrics on mobile phones is a possible direction that in the future could be an extension of the work we presented in this paper.

References

[1] J. Ashbourn, Biometrics in the New World, New York: Springer, 2014.

[2] A. K. Jain, A. A. Ross and K. Nandakumar, Introduction to Biometrics, New York: Springer, 2011.

[3] S. Yegulalp, "Computer World," 16 March 2011. [Online]. Available: https://www.computerworld.com/article/2506688/mobile-wireless/speech-recognition--your-smartphone-gets-smarter.html. [Accessed 23 October 2017].

[4] phys organization, "World's First Face Recognition Biometric for Mobile Phones," phys.org, 2005.

[5] C. Bhagavatula, U. Blase, K. Iacovino, M. S. Kywe, F. L. Cranor and M. Savvides, "Biometric Authentication on iPhone and Android Usability, Perception, and Influences on Adoption," in *USEC*, San Diego, 2015.

[6] R. Triggs, "Android Authority," 14 September 2017. [Online]. Available: https://www.androidauthority.com/facial-recognition-technology-explained-800421/. [Accessed 2 November 2017].

[7] J. Chakrabarty, "Fingerprint Scanner On Phones: History & Evolution, But Do We Really Need That?," iGadgetsworld, 2016.

[8] S. Rosenblatt, "iPhone 5S comes with Touch ID fingerprint scanner," cnet.com, 2013.

[9] C. Velazco, "Apple's Touch ID Is A 500ppi Fingerprint Sensor Built Into The iPhone 5S Home Button," techcrunch.com, 2013.

[10] A. Saxena, "iPhone 5S home button assembly picture suggests fingerprint scanner support," Gadgets360, 2013.

[11] C. Newton, "Apple's new iPhone will read your fingerprint," THEVERGE, 2013.

[12] N. Hughes, “Fingerprint sensor in Apple's 'iPhone 5S' predicted to boost mobile commerce, enterprise adoption,” appleinsider.com, 2013.

[13] shams, “List of All Fingerprint Scanner Enabled Smartphones,” webcusp.com, 2017.

[14] D. H. Cho, K. R. Park and D. W. Rhee, “Real-time Iris Localization for Iris Recognition in Cellular Phone,” in *Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks*, Washington DC, 2005.

[15] F. Okumura, A. Kubota, Y. Hatori, K. Matsuo, M. Hashimoto and A. Koike, “A study on biometric authentication based on arm sweep action with acceleration sensor,” *Intelligent Signal Processing and Communications,* no. 41, pp. 219-222, 2006.

[16] A. Hadid, J. Heikkila, O. Silven and M. Pietikainen, “Face and eye detection for person authentication in mobile phones,” in *Distributed Smart Cameras, 2007. ICDSC ’07. First ACM/IEEE International Conference*, 2007.

[17] H. A. Shabir and P. Suganthi, “Mobile phones security using biometrics,” in *Proceedings of the International Conference on Computational Intelligence and Multimedia Applications*, Washington, DC, 2007.

[18] J. Wang, Y. Li, P. Liang, G. Zhang and X. Ao, “An effective multi-biometrics solution for embedded devices,” in *ystems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference*, 2009.

[19] M. Conti, I. Zachia-Zlatea and B. Crispo, “Mind how you answer me!: transparently authenticating the user of a smartphone when answering or placing a call,” in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, New York, 2011.

[20] International Telecommunication Union, “ICT Facts and Figures,” ITU, 2014.

[21] Find Biometrics, “Find Biometrics,” 11 August 2017. [Online]. Available: https://findbiometrics.com/t-mobile-revvl-smartphone-408113/. [Accessed 2 October 2017].

[22] Apple, “Apple Inc,” iPhone X, 2017. [Online]. Available: https://www.apple.com/lae/iphone-x/. [Accessed 20 October 2017].

[23] S. Ruan, J. Wobbrock and K. Liou, “Speech is 3x Faster than Typing for English and Mandarin Text Entry on Mobile Devices,” *arvix.org,* 25 August 2016.

[24] Gartner, “Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016,” Gartner, Stamford, 2014.

[25] Acuity , “Biometric Smartphone Update,” Acuity Market Intelligence, 2106.

[26] Research and Markets, “Fingerprint Sensors Market in Smart Mobile Devices,” Research and Markets, 2015.

[27] M. Sahidullah, “Enhancement of Speaker Recognition Performance Using Block Level, Relative and Temporal Information of Subband Energies,” Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, 2015.

[28] C. García-Mateo, D. Petrovska and M. Tistarelli, “Biometrics for Secure Authentication,” Information Society Technologies, 2012.

[29] A. C. Weaver, “Biometric authentication,” *Computer,* vol. 39, no. 2, pp. 96-97, 2006.

[30] J. A. Bolle, M. Ruud and P. Sharath, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publications, 1999.

[31] A. Greenber, “Forbes,” 11 September 2013. [Online]. Available: https://www.forbes.com/sites/andygreenberg/2013/09/11/motorola-bashes-apples-iphone-fingerprint-reader-forgets-it-sold-one-first/#79efbb785e69. [Accessed 14 October 2017].