The 9th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, Serbia

SECURE MOBILE BANKING BIOMETRIC AUTHENTICATION

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade and eSigurnost Association, Belgrade, macek.nemanja@gmail.com

MILAN MILOSAVLJEVIĆ
Singidunum University, Faculty of Technical Sciences, mmilosavljevic@singidunum.ac.rs

IGOR FRANC
Belgrade Metropolitan University, Faculty of Information Technologies and SECIT Security Consulting, igor.franc@metropolitan.ac.rs

ZLATOGOR MINCHEV
Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences, zlatogor@bas.bg

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences, milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, btrenkic@viser.edu.rs

Abstract: *This paper presents an approach to securing mobile banking biometric authentication. The proposed system is based on secure client-server conventional XOR biometrics, which stores, transmits and verifies templates in encrypted form. Encryption keys are stored on bank's authentication servers, thus protecting the user twofold: if the phone gets stolen, both encryption keys and original templates are unavailable to an adversary. Once the user is authenticated, the communication between the client (the smartphone) and the server (bank) is encrypted. Having in mind that modern smartphones have iris scanners which operate by calculating Hamming distance and that variety of smartphones have fingerprint readers, which can, according to literature, be converted to XOR biometrics, one may conclude that the system is highly applicable and that it does not suffer from severe computational costs and drawbacks originating from cryptographic operations.*

Keywords: *Biometrics, Authentication, Cryptography, Mobile Banking*

1. INTRODUCTION

Mobile banking is a service provided by a financial institution that allows customers to conduct financial transactions, such as electronic bill payments and funds transfers, using a mobile device and software provided by the aforementioned institution. While mobile banking has it's upsides, security of financial transactions is a very important issue that needs to be addresed very carefully, as online banking is one of the most sensitive tasks performed by general user [1]. Althoug many traditional banks offer mobile baking with peace of mind [2], one should note that there is not a silver bullet providing a user with 100% security guarantee. According to [3], "a survey conducted by the Bureau of Financial Institutions found that 75 banks and credit unions' losses due to data security breaches reached a total of over $2.1 million US. This is a significant loss that financial institutions must address in order to reduce fraud rates and protect users worldwide." Jeon et al. identified three assets (which can be defined as targets of attack for mobile devices): device, application and private information [4]. Aforementioned authors defined a threat as anything that is capable of acting against an asset in a manner that can result in harm [4]. Broadly, two types of threats are identified in [5]: ones casued by external factors (adversaries) and ones caused by internal factors (user unawareness). Regarding financial transactions conducted via mobile the devices the following security apects should be addressed: physical security of the device, security of application running on the device, authentication of the user and the device to the service provider, encryption of data being transmitted and data that will be stored in device for later analysis by the customer.

Variety of authentication methods, both having upsides and downsides are implemented in mobile banking today. As an example, customers that secure data with passwords or PINs are at risk of fraud. Major companies have identified the need for strong security countermeasures and they are producing new hand-held products with built-in biometric devices. Accordig to [6], "the market size for biometrics is expected to reach $24.59 billion in the next six years and a lot of the growth will be seen from banks." According to Gartner, over 30% of mobile devices are currently using biometrics; banks should see as an opportunity rather than a barrier to adoption [7]. Although users of biometric devices do not need to remember passwords or carry tokens and biometric traits are distinctive and non-revocable in nature [8], thus offering

non-repudiation [9], one should note that biometric templates can be intercepted, stolen, replayed or altered if unsecured biometric device is connected to a network or if an adversary gains physical access to a device. This enforces the need for identity theft prevention with technological countermeasures such as cancelable biometrics, such as non-invertible transforms presented in [10, 11] and strong cryptography.

Research presented in this paper deals with authentication issue in mobile banking: precisely, cryptographically secure authentication based on conventional XOR biometrics presented in [12] is employed as mobile banking authentication system. Variety of smartphones having fingerprint readers, while devices with iris scanners are emerging technology. As fingerprint can be converted into XOR biometrics [13] and iris is verified by calculating Hamming distance and comparing it with a threshold, we can conclude that this modular system is suitable for implementation in mobile banking.

2. SECURED MODULAR AUTHENTICATION SYSTEMS WITH DISTRIBUTED STORAGE

In this section, cryptographically secured modular authentication systems based on conventional XOR biometrics with distributed storage are briefly described. Additional details on enrolment and verification phases as well as security evaluation of the system are given in [12].

System consists of one or more clients, an authentication server and a trusted storage. Client is a device used to capture biometrics, obtain auxiliary data and create encrypted cancelable templates. Authentication server manages encryption keys and verifies cancelable templates, while the trusted storage stores the encrypted templates. Two important characteristics of the proposed system are that it keeps biometric templates encrypted or cancelable during all stages of storage, transmission and verification, and that it does not suffer from severe computational costs and large sizes of encrypted templates.

3. IMPLEMENTATION IN MOBILE BANKING AUTHENTICATION SCENARIO

Authentication server resides in the bank. As authentication server stores encryption keys, it is logically that encrypted templates reside on the client. This prevents the attacker who obtains illegal access to authentication server to decrypt the temples.

The client is a mobile device (smartphone or a tablet) with fingerprint reader or an iris scanner. If the fingerprint biometrics is used, conversion to conventional XOR biometrics before cancellable template generation is necessary during both enrolment and verification phases. A system that generates XOR biometrics of fingerprints based on filterbank of Gabor filters of different spatial radial angles is presented in [13]. According to authors, the resulting fixed-length binary representation was tested in an authentication scenario with associated mechanism for extraction of associated cryptology keys, based on the principles of error correcting codes and the perspective of the proposed approach was experimentally evaluated. Additional software that provides feature extraction and cryptographic operations is installed on the client (as an additional application provided by the bank).

The non-invertible transform key is stored on the device. User obtains this key from the bank. User is allowed to wipe both the key and the data stored during enrolment phase both locally, if he suspects the data is somehow compromised, and remotely, if the device gets stolen. The bank is allowed to do remote data wiping also, if the authentication server is somehow compromised.

During the enrolment phase, client-side application calculates hash of the devices' IMEI and sends it to the authentication server. Server generates a private-public keypair (K_{priv}, K_{pub}), stores the private key with hash of IMEI (H(id), K_{priv}) and sends public key to the mobile device. User provides biometrics to the mobile device. Client-side app creates a binary template b_0 (with the aid of additional conversion if fingerprints are used) and generates cancelable binary template $b = K_t \oplus b_0$ using non-invertible transform key stored on the device. Client-side app further generates random seed s_0 and encrypts it with the public key: $s_E = E(s_0 , K_{pub})$. App generates a keystream $s = PRNG (s_0)$ using pseudorandom number generator and given seed, calculates $s \oplus b$, stores values (s_E, $s \oplus b$) on the device and discards the rest of the data.

During the verification phase, hash of the device IMEI is calculated on the client-side application and sent to the authentication server. User provides biometrics to the mobile device. Client-side app creates template b_0' and generates cancelable binary template $b' = K_t \oplus b_0'$. App retrieves values s_E and ($s \oplus b$), calculates $s \oplus b \oplus b'$ and sends it with the encrypted seed s_E and hash of the devices' IMEI to the authentication server. Server retrieves private key from stored record (H(IMEI), K_{priv}) with the corresponding device IMEI hash, decrypts the seed with the private key $s_0 = E(s_E , K_{priv})$ and generates the keystream: $s = PRNG (s_0)$. Authentication server calculates $b \oplus b' = s \oplus s \oplus b \oplus b'$ and compares the Hamming distance between cancellable templates b and b' with the treshold. According to that result, the decision is made and sent back to the client. If the user is genuine, the rest of the communication between the mobile device and mobile banking authentication server is encrypted.

4. SECURITY OF THE PROPOSED SYSTEM

Regarding the security of the proposed solution, the following conclusions can be made. Templates are encrypted or at least cancelable during all stages of storage, transmission and verification, and the mobile device is not allowed to access private keys stored on authentication server. Authentication server has no access to the transform keys and cancellable templates created on the mobile device during enrolment. If the phone is stolen, an adversary cannot claim as legitimate user as the system is prone to all attacks listed in [14] as well as to hill-climbing, non-randomness, re-usability, blended substitution and linkage attack. Additionally, one should note that the user is allowed to remotely wipe all stored data if the phone gets lost or stolen.

However, one should note that security of the system also depends on the security of the biometric device itself. As

an example, a hack on Samsung Galaxy S8 iris scanner is briefly discussed. Iris patterns stable and distinctive features for personal identification [15]. More than 250 distinguishing characteristics of an iris (degrees of freedom) can be used in biometrics, resulting in six times more identifiers than the fingerprint [16]. This is why iris is sometimes referred to as an optical fingerprint. According to aforementioned, iris scanners should be hard to trick into false acceptance, but a group of hackers have managed to do so with the iris-based authentication in Galaxy S8 in an easy-to-execute attack. Hardware required to complete the attack included a digital camera, a printer and a contact lens, costing less than the unlocked smartphone. The hack required taking a picture of the subject's face, printing it on paper, superimposing the contact lens (see Image 1), and holding the image in front of the locked phone [17].

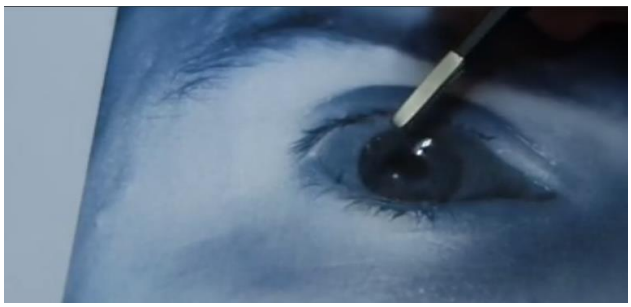

Image 1: Galaxy S8 iris-based authentication hack (still-frame taken from [18])

Despite that, the manufacturer of the iris recognition used in the smartphone still claims that iris recognition allows consumers to finally trust that their phones are protected.

CONCLUSION

This paper presented an implementation of modular authentication systems based on XOR biometrics into mobile banking. Security evaluation of the proposed system given within the paper. According to high level of security and low computational costs make it highly applicable as an authentication solution for mobile banking. Our further work will focus on implementing the system in simulated mobile banking scenario.

REFERENCES

[1] M. Mannan and P. C. Van Oorschot, “Security and Usability: The Gap in Real-World Online Banking”, NSPW’07, North Conway, NH, USA, Sep. 18-21, 2007.

[2] Y.S. Lee, N.H. Kim, H. Lim, H. Jo, and H.J. Lee, “Online banking authentication system using mobile-OTP with QR-code”, in Proc. 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), 2010, November 2010, pp. 644-648, IEEE.

[3] B. Armour, “Biometric Authentication for Mobile Banking: What Banks Need to Know”, Clear Bridge Mobile, available online, last time visited September 2017.

[4] W. Jeon, J. Kim, and Y. Lee, Y., “A practical analysis of smartphone security”, Human Interface and the Management of, 6771, pp. 311-320, 2011.

[5] I. Ashra, “Mobile Banking Security”, Vrije Universiteit, Amsterdam, Thesis number 1073, April 2012.

[6] B. Armour, “How Biometric Authentication is Shaping the Future of Mobile Banking”, Clear Bridge Mobile, available online, last time visited September 2017.

[7] C. Stamford, “Gartner Says 30 Percent of Organizations Will Use Biometric Authentication for Mobile Devices by 2016”, February 4, 2014, available online, last time visited September 2017.

[8] Y. C. Feng, P. C. Yuen and A. K. Jain, “A Hybrid Approach for Face Template Protection”, in Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, pp. 325, 2008.

[9] P. Balakumar and R. Venkatesan, “A Survey on Biometrics-based Cryptographic Key Generation Schemes”, International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.

[10] N. K. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, “Generating Cancelable Fingerprint Templates”, Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), pp. 561-572, 2007.

[11] J. Zuo, N. K. Ratha and J. H. Connell, “Cancelable iris biometric”, In Pattern Recognition, ICPR 2008, 19th International Conference on (pp. 1-4), IEEE, 2008.

[12] N. Maček, M. Milosavljević, I. Franc, M. Bogdanovski, M. Gnjatović and B. Trenkić, “Secure Modular Authentication Systems Based on Conventional XOR Biometrics”, accepted for publication in The 9th International Conference on Business Information Security Proceedings.

[13] S. Barzut and M. Milosavljević, “Jedan metod formiranja XOR biometrije otisaka prstiju Gaborovom filtracijom,” in Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide, Belgrade, Singidunum University, Serbia, 2014, pp. 610-615.

[14] R. Jain and C. Kant, “Attacks on Biometric Systems: An Overview”, International Journal of Advances in Scientific Research, 1(07), pp. 283-288, 2015

[15] S. Lim, K. Lee, O. Byeon and T. Kim: “Efficient iris recognition through improvement of feature vector and classifier”. ETRI journal, 23(2), pp. 61-70, 2001.

[16] G. Amoli, N. Thapliyal and N. Sethi, “Iris Preprocessing”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 6, pp. 301-304, 2012.

[17] D. Goodin, “Breaking the iris scanner locking Samsung’s Galaxy S8 is laughably easy”, Ars Technica, May 23, 2017, available online, last time visited September 2017.

[18] Hacking the Samsung Galaxy S8 Irisscanner, online: https://media.ccc.de/v/biometrie-s8-iris-en#video&t=66, last time visited September 2017.