Smartphone as a Biometric Service for Web Authentication

Regio A. Michelin*, Avelino F. Zorzo§, Marcia B. Campos¶, Charles V. Neu† and Alex M. S. Orozco‡
*Federal Institute of Rio Grande do Sul (IFRS), †University of Santa Cruz do Sul (UNISC),
‡Sul-rio-grandense Federal Institute (IFSul), *†‡§¶Pontifical University of Rio Grande do Sul (PUCRS)
Email: *regio.michelin@restinga.ifrs.edu.br, §avelino.zorzo@pucrs.br,
¶marcia.campos@pucrs.br, †charles1@unisc.br, ‡orozco@sapucaia.ifsul.edu.br

Abstract—**Authentication is a crucial solution to be considered for securing an application or user's personal data. It is a mechanism that plays a role to allow only the rightful user to access an application and the corresponding data, without allowing any kind of impersonation. To avoid this impersonation, biometric mechanisms have been used to read some biological characteristic from the user. However, the extra hardware needed for reading the biometric feature is usually a problem. Besides, in some scenarios, this will definitely avoid its adoption. Nonetheless, nowadays, this problem may be reduced since almost every adult person possesses a smartphone, which contains several sensors that can be used to read biometric information from a user. This work proposes a mechanism to allow a smartphone to act as a biometric reader for different levels of task/data available in a web application. In order to bind a smartphone to a web application, we use QR-Code sent from a web server to a web client, which will have to be read by a smartphone and then be sent back to the web server, so the web server knows that the actual user is close to the web client. This paper also provides a discussion on how to evaluate the usability of the proposed mechanism.**

Index Terms—**Usability, Authentication, Security, Two Factor, Continuous Authentication, Biometrics**

I. Introduction

To create an online account is a trivial operation performed by almost all Internet users. Every day new accounts are created to online banking, shopping, email, social networks, news forum, and so on. For each created account, every user is prompted to associate a unique identifier (its username) and a secret key (password) that will be used to give access to this account only to the rightful person. In 2007, web users had an average of 25 online accounts that require password usage, and they are prompted around 8 times per day to enter these passwords[1] [1]. Not only the amount of accounts is a problem, but in order to choose a good password the user has to include upper and lower case characters, digits and special characters, avoid characters repetition and the password must avoid using dictionary words [2]. Despite of that, there is a recommendation to change passwords from time to time, to a new one, following the same policy.

Since the users are overwhelmed to be compliant with these password policies, they usually choose to use low quality passwords that will facilitate the unauthorized access to their online accounts. A lot of research has been performed lately in order to provide new authentication mechanisms that avoid this user information overload [3] [4] [5]. In the recent year, the use of biometry [6] has increased, since its concept is based on reading some unique biological information (visual, voice, gesture, finger print, etc) from the user, an information that cannot be easily stolen. Again, the main goal is to allow only legitimate users to access a system. However, the use of biometry is a problem since not every computer includes a sensor to read biological information from the user, and, therefore, an extra hardware would have to be acquired.

Since nowadays almost every person possesses a smartphone, this extra hardware requirement becomes unnecessary. These smartphones are usually equipped with sensors, such as camera, GPS, accelerometer, fingerprint reader, etc. Based on the smartphone popularization and its capability of reading different biometric information through sensors, this research proposes to use a smartphone as a hardware to read user's biometric information in order to propose an alternative to conventional passwords. Through this approach, even if the computer is compromised, the smartphone can use a different communication channel to send the user information to a web server, for example.

The authentication proposal will be evaluated in a field study, in order to get users feedback and raise usability concerns. This usability aspect can be evaluated in a quantitative and qualitative ways. The authentication mechanism usability has to be evaluated, to ensure that it will be ease to use. Keith [7] research, for example, shows that when a mechanism does not present good usability, the user tends to use a different mechanism, which sometimes lead to reduce its account security.

The remain of this paper is organized as follows. Section II presents some related work that help understanding the current trends and challenges on biometric authentication. Section III describes the proposed biometric authentication using a smartphone and web applications. The mechanism evaluation is discussed in Section IV focusing on its usability, as well as, not impacting application security. Section V brings the future directions that are being performed in order to achieve this research goal.

[1] In this work, we are going to use "conventional password" to the ones in which a user has to type a set of characters.

978-1-908320/73/5/$31.00 © 2016 IEEE

TABLE I
EXISTING USER AUTHENTICATION METHODOLOGIES [4]

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

II. BACKGROUND AND RELATED WORK

A survey of biometric authentication mechanisms applied to mobile phones was presented by Meng [4]. In that survey, there is a classification that defines two different techniques applied to biometrics: physiological, which is basically the measurement of some human body characteristic; and, behavioral, which is related to the reading of information produced by a human user (see Figure 1). The definition of three main classes of authentication mechanisms is presented in Table I. These classes are divided by what the user knows, have or is, and from the possible authentication mechanisms. From these classes, using the representation of what the user is, is the only one that cannot be shared and even repudiated. Despite of this advantage, its trade off is the usability problem that is raised due to the need of extra hardware to retrieve the information, and its accuracy, which despite of research being performed lately, there exist some vulnerable situations in which false positives ore negatives can be generated, *e.g.* using face recognition could generate a false positive since a picture of the user could be used in front of the camera (there are some techniques to avoid that); or if the user is wearing sunglasses, the users do not be recognized (false negative).

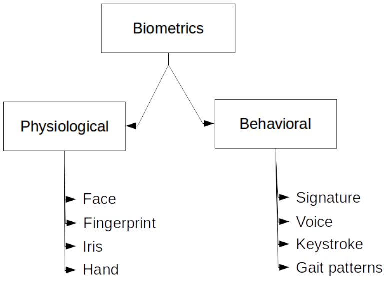

Fig. 1. Biometric classification adapted from Meng.

Some mechanisms to use mobile authentication have already been proposed. For example, Crawford [3] proposes a mechanism based on different levels access for sensitive information, for example, accessing home banking needs a higher level of security than reading news in a web site. Even in the same server, different levels of security might be necessary, *i.e.* home banking. So to manage these different levels of sensitive information, a scale from zero to one was defined. Where zero value in the scale means a task that requires no or low authentication level, on the other hand, one means a high level of authentication. The mechanism starts on a training mode, where its value is set to 0.5. During this period of time, the mechanism learns the user preferences and patterns in order to identify his behavior. Once the training session has finished, a user pattern is stored and all new operations will be authenticated based on the stored pattern. After that, if the user pattern deviates from the original pattern, user will be asked to authenticate again. Besides, after the user authentication using username and password, the authentication level may reduce until it reaches a certain threshold when he will have to authenticate again. This authentication level reduction is time based. The information gathered from a user, is applied in order to trace his behavior. Basically the mechanism of transparent authentication keeps the time, user information and the probability of an event occur, this event could be opening an application, reading some email, etc.

Another important point that has to be analysed when using biometry, is to measure its usability from a user perspective. Tassabehji [8] proposed a biometric mechanism that is applied to e-banking authentication, and to evaluate its usability the System Usability Scale (SUS) [9] was applied. The biometry was applied in an e-banking application to increase the user security perception, as well as, improve its usability. SUS is a usability scale for assessments. This scale is composed by ten items of subjective assessments of usability; it is based in a Likert scale. This scale uses a five or seven points in which the user chooses his degree of agreement with some of ten statements. All affirmations are related to the software usability and gives a quantitative value from the users answers. SUS questions that will be applied in a questionnaire [9]: 1) *I think that I would like to use this system frequently;* 2) *I found the system unnecessarily complex;* 3) *I thought the system was easy to use;* 4) *I think that I would need the support of a technical person to be able to use this system;* 5) *I found the various functions in this system were well integrated;* 6) *I thought there was too much inconsistency in this system;* 7) *I would imagine that most people would learn to use this system very quickly;* 8) *I found the system very cumbersome to use;* 9) *I felt very confident using the system;* 10) *I needed to learn a lot of things before I could get going with this system.*

In order to retrieve more accurate information, a qualitative questionnaire will also be conducted with users that will use the authentication mechanism.

III. AUTHENTICATION MECHANISM ARCHITECTURE

This section describes the system architecture and its operation. The system's main idea is to use a smartphone as a biometric reader and thus replace conventional password. As a proof-of-concept (POC), we have implemented a tool for the Android OS. This POC brings a native face recognition mechanism that is used by this OS to unlock the smartphone replacing the gesture or PIN [10], and in this case the camera is used as a sensor to read the user image.

Figure 2 shows a high level architecture of our proposal. First and foremost, it is important to mention that there exists a bootstrap phase, that we do not describe in this paper. After that, once the user, through a computer running a web client, wants to access a web server, first he must inform who he is (step 1). Based on that, the web server generates a hash based on the user information and a time stamp, according to Listing 1. This hash is sent from the web server to the web client (step 2), and it will display a QR-Code that represents this hash. The user through his smartphone must scan the QR-Code (step 3), this step is performed to the ensure that the user is physically located at same place that the computer is (step 4). Once this step is performed, the smartphone can be also considered as a hardware possessed by user, and from now on it will act as a biometric reader.

Listing 1. QRCode generation.

```
QRCode=Hash(username, server timestamp,
   ↪ salt);
```

The web server, which will be responsible for sending the QR-Code to the web client and also analyzing the user biometric information, is an implementation algorithm based on Crawford [3] continuous and transparent authentication framework. It is responsible to evaluate the user behavior, based on the navigation and tasks executed on the web client. Each time that a new authentication is required, depending on data sensitiveness or task, the user will be prompted to execute some biometric reading (steps 5 and 6).

Listing 2. Smartphone biometric sensor enumeration.

```
SensorList=[KS – Keystroke, SG – Signature
   ↪ , VC – Voice, FP – Fingerprint, FC –
   ↪ Face, IR – Iris, GT – Gait];
```

Since most smartphones are equipped with several different sensors, and considering that each biometric mechanism has some weakness, once the communication is established (through QR-Code reading), the smartphone provides to web server a list of all available sensors (see Listing 3), that could be used in order to perform the user biometric reading. So from this list (see Listing 2) the web server is able to sort it by its reliability and according to the data sensitiveness management, a biometric reading will be prompted.

Listing 3. Binding Smartphone.

```
SmartphoneBinding=SendingToServer(username
   ↪ , hash, geoLocation, SensorList [KS,
   ↪ SG,VC,FP,FC,IR,GT]);
```

In order to trace the user behavior, information is gathered from the computer and from the mobile device to ensure the user is who he says he is. Based on this behavior, the web server can ask for a new biometric reading (from the mobile device). This action will be triggered to ensure that the user still has the smartphone. The system can also ask the user to scan a new QR-Code, to prove that the user is still in the same place the computer is.

Table II [4] [6] presents a summarized analysis of biometric mechanisms. Table II is used to define the order of sensors that the web server is going to use to collect some biometric feature. Furthermore, depending on how sensitive the information is, or which system is being accessed, the web server can choose a more or less accurate biometry. Naturally, the web server can also use information about error incidence for each characteristic when analysing the authentication provided by the user. For example, if face recognition is being used and the user is using glasses, this could be identified by the system, and a message could be sent to the user in order for him to send an image without glasses, or a different sensor could be activated for that authentication.

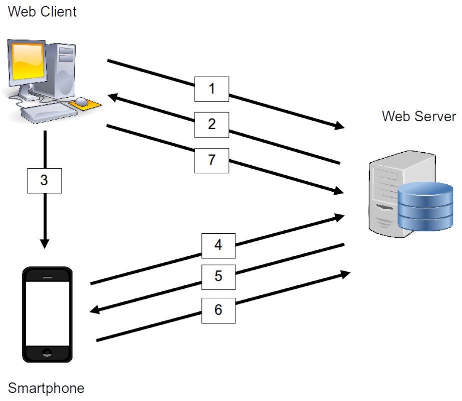

Fig. 2. Proposed authentication architecture

IV. Discussion

This section provides some discussion on the possible issues and benefits that the proposed mechanism will provide regarding the security and usability in comparison to conventional password usage.

Applying our proposed mechanism, through biometric reading, we are willing to minimize the possible user impersonation, as well as, the problems related to conventional password memorability. Furthermore, it is also possible to considerably reduce attacks, for example, shoulder surfing attacks, which represent a very common vulnerability related to conventional password, or even to graphical passwords [11].

Another benefit from our proposal is that we can ensure that the user (or at least his smartphone) is located in the same place as the web client that is accessing the web server. This is guaranteed since the QR-Code shown in the web client screen has to be read by the camera in the smartphone that is bind to a specific user. At this moment we do not consider relay attacks, *i.e.* the possibility that another user captures the image from the web client, sends this image to the real user, that in turn, uses his smartphone to send the correct authentication to the web server. This situation could also be avoided using some timing strategy or using GPS information about the web client and the smartphone.

As mentioned in Section III, the web server can provide different levels of data or system sensitivity. Based on these different levels of sensitivity, the web server can keep asking for authentication any time the user (web client) wants to access a different system or information. This can run similarly to token authentication from banks when, after you authenticate to use your bank account, depending on the operation you are performing, it may ask for a new token or even a different information.

TABLE II
COMPARISON OF BIOMETRICS ADAPTED FROM [4] [6]

Characteristic	Fingerprint	Face	Voice	Signature	Iris	Gait
Ease of use	High	Medium	High	High	Medium	Medium
Accuracy	High	High	High	High	Very high	Low
Error incidence	Dryness, dirt, age	Lighting, age, glasses	Noise, colds, weather	Changing signatures	Poor lighting	Terrain, injury

In order to evaluate the authentication mechanism usability in a qualitative perspective, we intend to use a questionnaire that follows nine aspects [12]: efficiency (*e.g.* does the mechanism provide access to the system only to rightful users?), satisfaction, productivity, learnability (*e.g.* does the mechanism allow a user to learn how to use the system without a lot of effort?), safety (*e.g.* does the mechanism provides error treatment?), trustfulness, accessibility (*e.g.* does the mechanism allow disabled user to access a system?), universality and usefulness (*e.g.* does the mechanism provides different ways to access a system?). All these aspects will be considered from a web application perspective as well as from a biometric reader perspective.

V. CURRENT WORK AND CONCLUSION

As this is a work-in-progress research, we still need to finish the POC and then start assessing functionality and usability with real users. As a criteria to choose volunteers, due to implementation limitation, they will have to use a smartphone that runs the Android OS. In order to retrieve the information related to issues and mechanism usability, the volunteers will answer a questionnaire based on SUS, and they will be monitored during the test, which will be performed for a period of three months. We intend to evaluate the number of explicitly authentication performed during system usage, and also measure the False Acceptance Rate (FAR), which is the percentage of impostors incorrectly matched to a valid user biometric, as well as, False Rejection Rate (FRR), *i.e.* the percentage of incorrectly rejected valid users. In order to finally assess the usability, we intend to use a different questionnaire asking the user more qualitative information about the system usage. Through monitoring the mechanism usage and conducting questionnaires, we intend to identify the users expectation before the mechanism usage, and also after the conducted test.

It is important to mention that our mechanism also provides an option so the user can reduce, or even disable, the level of security, based on the biometric authentication that is provided. This will provide the user to return to the conventional user/password authentication mode. In order to understand the reasons that drove the user to perform this change, we intend to prompt the user with the possibility to explain why he has chose to return to the conventional user/password authentication. This will provide feedback, so we can improve our mechanism.

There has been some work [13] in the past that proposes a framework for online bank application, where it combines a user smartphone, a web client, the bank application, and a certification authority. The proposed framework is based on an One Time Pad (OTP), which is generated in the web client and shared to the smartphone through QRCode. Once this OTP is read by the smartphone, it is sent to the certification authority for validation. This strategy is different from ours, since it has an extra step, *i.e.* the use of a certification authority, and does not use biometry to authenticate a user.

REFERENCES

[1] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th International Conference on World Wide Web*, ser. WWW '07. New York, NY, USA: ACM, 2007, pp. 657–666. [Online]. Available: http://doi.acm.org/10.1145/1242572.1242661

[2] A. Bafna and S. Kumar, "ProActive Approach for Generating Random Passwords for Information Protection," *Procedia Technology*, vol. 4, pp. 129–133, 2012. [Online]. Available: http://dx.doi.org/10.1016/j.protcy.2012.05.018

[3] H. Crawford, K. Renaud, and T. Storer, "A framework for continuous, transparent mobile device authentication," *Computers and Security*, vol. 39, no. PART B, pp. 127–136, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2013.05.005

[4] W. Meng, D. S. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1268–1293, 2015.

[5] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *Proceedings - IEEE Symposium on Security and Privacy*, pp. 553–567, may 2012.

[6] S. Liu and M. Silverman, "Practical guide to biometric security technology," *IT Professional*, vol. 3, no. 1, pp. 27–32, 2001.

[7] M. Keith, B. Shao, and P. J. Steinbart, "The usability of passphrases for authentication: An empirical field study," *International Journal of Human Computer Studies*, vol. 65, no. 1, pp. 17–28, 2007.

[8] R. Tassabehji and M. a. Kamala, "Evaluating biometrics for online banking: The case for usability," *International Journal of Information Management*, vol. 32, no. 5, pp. 489–494, 2012. [Online]. Available: http://dx.doi.org/10.1016/j.ijinfomgt.2012.07.001

[9] J. Brooke, "SUS - A quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996. [Online]. Available: http://hell.meiert.org/core/pdf/sus.pdf

[10] R. D. Findling and R. Mayrhofer, "Towards face unlock: on the difficulty of reliably detecting faces on mobile phones," *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia - MoMM '12*, p. 275, 2012. [Online]. Available: http://dl.acm.org/citation.cfm?id=2428955.2429008

[11] F. Tari, A. A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proceedings of the Second Symposium on Usable Privacy and Security*, ser. SOUPS '06. New York, NY, USA: ACM, 2006, pp. 56–66. [Online]. Available: http://doi.acm.org/10.1145/1143120.1143128

[12] C. Braz, A. Seffah, and D. M'Raihi, *Designing a Trade-Off Between Usability and Security: A Metrics Based-Model*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 114–126. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74800-7_9

[13] Y. S. Lee, N. H. Kim, H. Lim, H. K. Jo, and H. J. Lee, "Online Banking Authentication system using Mobile-OTP with QR-code," *Proceeding - 5th International Conference on Computer Sciences and Convergence Information Technology, ICCIT 2010*, pp. 644–648, 2010.