Telecommunication Systems (2018) 69:365–379
https://doi.org/10.1007/s11235-018-0437-1

User perspective and security of a new mobile authentication method

Pawel Laka[1] · Wojciech Mazurczyk[1]

Published online: 16 March 2018
© The Author(s) 2018

Abstract

This paper describes a new mobile authentication method which is based on an Open ID Connect standard and subscriber identity module card. The proposed solution enables users to access websites, services and applications without the need to remember passwords, responses or support of any equipment. The proposed method is evaluated from the users' perspective as well as from the security viewpoint. Moreover, we compare it with the two most popular existing authentication schemes i.e. static passwords and SMS OTP (one time password). In order to evaluate user's view on various authentication methods a questionnaire was prepared and distributed among 40 participants. Obtained results revealed that the new authentication scheme yielded better results than the existing methods. Finally, we also performed a security analysis with respect to all abovementioned authentication solutions to assess whether there are any major risks related to the proposed method.

Keywords Authentication convenience · Smart cards · Security · User experience

1 Introduction

Along with the dynamic development and utilization of the self-care services, such as banking, e-commerce, healthcare, or e-government, there has been an increasing demand to properly authenticate users in a secure manner. It is vital to authenticate users as currently almost 46% of the global population has access to the Internet [1] and cybercriminals impersonate legitimate users, conduct frauds and steal data on a daily basis.

Despite many attempts to improve security in the communication networks, it is still humans that are the weakest link in the security chain. Fortunately, the awareness of online privacy and security protection among the network users is slowly awakening. One of the most common fears of Internet users is an identity theft attack. However, in most cases users are not fully aware of its risks and causes since they simply lack experience in the field of network security, which prevents them from protecting themselves effectively. Typically, users do not know basic means that can be used in order to protect one's identity. On the other hand, most well-known and common authentication methods are quite troublesome especially for the end users who represent low level of technical skills.

In general, current authentication processes rely on:

- something the user knows (e.g. static passwords, PIN, challenge questions etc.);
- something the user has (e.g. smart cards, hardware tokens, immobilizers etc.);
- something the user is (e.g. biometrics such as fingerprints, face or voice recognition, keystroke dynamics etc.).

The password-based authentication relying on something the user knows is probably the oldest and still most commonly used user authentication method. On one hand it is utilized very often, but on the other hand rarely used properly. For example, nowadays, it is common knowledge that static passwords should be long, complex and should not be reused between various services and providers that the user utilizes. But from the users' perspective such an approach is typically overcomplicated and annoying to apply in practice. This, in turn, leads to the point where people typically use simple and easily guessable passwords that can be broken with a (very basic) dictionary attack.

The main negative aspect of the methods that rely on something the user has is that the authentication process requires

✉ Pawel Laka
paul.pradera@gmail.com; plaka@tele.pw.edu.pl

Wojciech Mazurczyk
W.Mazurczyk@tele.pw.edu.pl; wmazurczyk@tele.pw.edu.pl

[1] Faculty of Electronics and Information Technology, Institute of Telecommunications, Warsaw University of Technology, 15/19 Nowowiejska Str., 00-665 Warsaw, Poland

the user to carry appropriate equipment with them. Moreover, for example in the smart vehicle scenario it may happen that, for instance, when the user is near his car with an immobilizer the car opens without the owner being aware of it.

Finally, the weakness of popular biometric systems (something that user is) consists in poor coping with changes. In case of stealing a fingerprint, a face shape or a scan of retina, the user cannot replace it with another one that was not previously stolen. Another thing is that people tend to leave this kind of data everywhere.

From another perspective, multi-factor authentication that combines all above mentioned methods is desirable in order to obtain desired Level of Assurance (LoA) defined by ISO/IEC 29115. The aim of multi-factor authentication is to enhance the strength of the authentication process. It usually increases the security level, especially if the authentication method forms a hybrid of what the user has, knows and is. Still, it should be noticed that a high LoA is not required in all cases. There is no point in using all authentication possibilities everywhere, especially if raising a number of authentication factors affects the user's perception. Unfortunately, it seems to be a rule that the more effective the confirmation of one's identity is (thus successful attacks are less probable), the less comfortable it is for the user.

On the other hand, designed authentication methods should not be susceptible to user errors. Therefore, the interaction between the user and the log in process should be prepared in a way so that it has both secure and user-friendly (ergonomic) authentication process.

Considering above, the aim of this paper is to evaluate the proposed mobile authentication method from the user perspective as well as from the point of view of security. Therefore, we focus both on user's comfort and security. The novel solution described in this paper is based on what the user has. Mobile phones with the Secure Element (SE), such as a smart card based on UICC (Universal Integrated Circuit Card), usually called just a 'SIM (Subscriber Identity Module) card', are almost omnipresent. SIM card seems to be a perfect carrier to provide authentications and digital signatures in a user's everyday life. Nowadays, carrying a mobile phone is not problematic for its user. To increase security the authentication process is based on a SIM card, and not only on security relying on the applications and the operating system. The proposed solution enables users to access websites, services and applications without the need to remember passwords, responses or a support of any equipment. The described method is based on a low LoA, which is still easy to be increased by adding more authentication factors, while utilizing the same idea. Considering the above, the main contribution of this paper is to demonstrate an innovative authentication solution that focuses on the usage that is at the same time comfortable and secure. This new authentication method was designed, developed and evaluated in comparison with other most common methods.

The rest of the paper is structured as follows. First, the related work in the field authentication of mobile users (chapter 2) is reviewed. Chapter 3 describes in detail the new authentication model and the corresponding remote architecture. In the next section (Sect. 4) an experimental methodology to capture user perspective is outlined. Obtained results of the aforementioned studies are shown in Sect. 5. Section 6 is devoted to security analysis of the proposed solution including potential risks and attacks identification and how to protect against them. Finally, Sect. 7 concludes the work.

2 Related work

A growing body of evidence clearly demonstrates that there is a problem to identify mobile users on the Internet. There are many works that deal with this topic, such as [2], which proposes an ID-based communication framework, where IP addresses play a significant role, not only in locating hosts and in routing the traffic, but also in the identification of hosts and services. In this paper, we adopt a MSISDN-based (Mobile Station International Subscriber Directory Number) user's identity. This allows finding the mobile device (SIM card) quickly while maintaining the integrity and the uniqueness. But in the future any other identifier can be chosen for this purpose.

Many studies have proposed an innovative authentication schemes based on different assumptions. One of the several possibilities are MAI (Message Authentication Image) [3] or other intelligent image-based authentication framework that falls under the "What you know" type of authentication [4]. Moreover, the article [5] proposes an authentication system using OTP (One Time Password) or QR codes (Quick Response Code). Papers [6] and [7] rely on a certificate-based authentication. The exchange of certificates is done on the basis of asymmetric encryption while the digital certificates are issued by a certification authority (CA). However, these works add the additional aspect which requires user attention. Thereby the convenience of the authentication process is lowered.

In order to secure mobile devices against different threats, biometrics has been applied. It seems to be a very effective way of authentication. In the last years, research has provided ample support for the assertion that biometrics is the future of authentication. There are plenty of works based on fingerprint [8], gait, face, voice, gesture, iris, typing pattern, signature [9] or even electrocardiograms acquired by mobile sensors [10]. All these solutions use an authentication method based on the data about "what user is". There are also works in the field of Wireless Sensor Network, where sensors are either attached to or embedded in the human body and communicate wirelessly with each other and with other components such as network towers, processors, servers, etc. [11]. It must be admitted that biometrics uses a very convenient way of authentication. However, in this paper, we focus on a single factor authentication, but any biometrics method could be developed in order to add another factor utilizing the described idea. Although, for now, due to many frauds and data leaks, biometrics was left for future work. The weakness of biometrics is that in case of data leakage we cannot change it, and this type of personal data can be left everywhere. Furthermore, biometric mobile applications are vulnerable to some types of attacks that can decrease their security [12]. Evidence presented in [12], which is based on the research into facial and fingerprint mobile authentication applications, shows that such mobile applications are vulnerable to several attacks, which poses a serious threat to the overall system security and user privacy.

In this paper, we focus on authentication method that relies on something the user has, meaning the SIM card. A lot of works have focused on such authentication [13–21]. They propose a SIM based protocol as an authentication tool over existing GSM technology through GPRS [14], for SIP [15,16]. Other papers describe an anonymous remote user authentication with a key agreement scheme based on smart card using chaotic maps [17] or other cryptographic operations [18–21]. There are several methods that provide user anonymity and traceability with solutions based on mobile cloud networks [22,23]. Unfortunately, all the papers mentioned above consider the secure exchange of information between the mobile device and the servers, and do not analyze human users' perspective. That is why, this paper focuses on introducing the authentication method which is both comfortable and safe. Security is an important matter; however, user convenience should be taken into consideration as well.

According to paper [24], which focuses on how to create an end-to-end secure channel between the digital services, the biggest open issue is how to design the user interaction in terms of data input and output in a way that users can reliably and unobtrusively be aware of which application part they are communicating with. Paper [25] pays greater attention to this issue. In this work, however, the solution is mainly described in terms of Man-in-the-middle (MitM) attack and is not based on standards.

There has also been research into the perception of users. Such studies are mostly done with the use of a survey questionnaire [26]. Evaluation of different authentication methods has been performed in the paper [27]. Three devices in the generation of one-time passcodes (OTPs) were compared. But only hardware tokens which are an additional device for the user to carry were included. Very precise research in this area is conducted in locking the smartphone screens [28]. Also, a questionnaire was used which was distributed among the users via online and offline means. Unfortunately, only widely used methods were evaluated, which allowed investigating a greater number of respondents. However, in this paper we present a method which is not yet available for the users widely.

To summarize, in contrast to the existing works mentioned above in this paper we propose a novel authentication method and we evaluate it in terms of user comfort and security. Moreover, we conduct its comparative analysis with two well-known existing solutions i.e. static passwords and SMS OTP (One Time Password).

3 System architecture

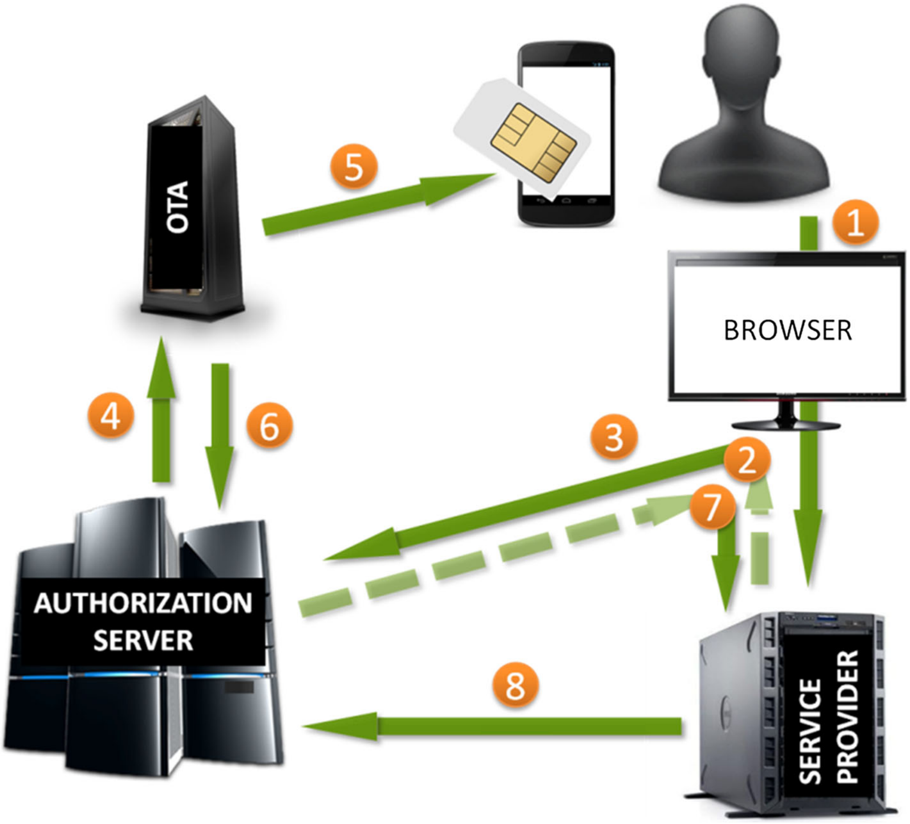
The purpose of the solution proposed in this paper is to provide a secure and user-friendly authentication method designed for mobile web applications of any service provider. In fact, the solution used here enables both: authorization and authentication of the end users. The main idea is to push a selection form to the user's mobile device to establish whether the user would like to be authenticated or not. In order to achieve this, an applet on the SIM card has been used. In this work, a standard applet was utilized, installed on the SIM card of one of the Polish mobile operators. The user, having provided only a login name to any website authentication form, is prompted to confirm the authentication process on their mobile device with a SIM card. After successful confirmation he is automatically redirected to the website he wanted to log in.

The log in process is based on an OpenID Connect standard [29] which is a simple identity layer on top of the OAuth 2.0 protocol [30]. OpenID Connect standard has been chosen as the base protocol and framework because of its openness and robustness. It can work on almost any device that has a web browser with access to the Internet. It works regardless of the operating system of the device. The OpenID Connect Specification is set by the OpenID Foundation, and is constantly evolving.

The proposed solution consists of four types of components, each performing different well-defined functions (Fig. 1):

- *Authorization system* This back-end system is used to provide a sign-on mechanism. The authorization system is responsible for handling users' data. In this work the LDAP was used as a database which contains users' credential information. In order to ensure security of the transferred data, communication channels are secured with HTTPS.
- *Over the air (OTA) system* OTA is a standard for the transmission and reception of the application-related information in a wireless communications system. OTA

Fig. 1 The logging process



is commonly used in conjunction with the Short Messaging Service (SMS), which allows the transfer of small text files. For the purpose of this work the mobile operator OTA server was used. OTA messages are encrypted to ensure user privacy and data security. In this solution the class 0 SMS has been used. In the mobile signature solutions, the mobile operator establishes communication with the secure element (SIM card) remotely (using encrypted SMS messages) bypassing the mobile terminal.

- *Applet deployed on a SIM card* Its purpose is to receive the requests from OTA. The interface with a SIM card is based on the SIM Application Toolkit (commonly referred to as STK). It is a standard in the GSM system which enables the SIM to initiate actions that can be used for various value-added services. STK requests are implemented differently on different operating systems, which will be described further in detail in the Sect. 6.3.
- *Service provider* Any external application developed in a technology that allows the usage of Authorization System. It may be a web application (from a bank, e-commerce etc.) where it is necessary to authenticate the user. Such applications should redirect the user to the Authorization System.

Protocols between the components are characterized as follows: HTTPS—in communication between Browser-Service Provider, Service Provider-Authorization Server, Browser-Authorization Server; WML and HTTPS—in communication between OTA and Authorization Server; Encrypted messages—between OTA and SIM card; STK push—between a SIM card and Mobile device screen which will be described thoroughly in Sect. 6.3.

The process of logging into the web application from the user perspective has been presented in Fig. 1.

The detailed flow of the logging into the external application integrated with the Authorization System using described method is as follows (Figs. 1, 2):

1. First, the user tries to enter the Service Provider site via a web browser. The user clicks “Log in” in the web application in order to access the service (phase 1).
2. Then, the Application makes an authentication request to the Authorization Server using OpenID based on OAuth 2.0 and redirects user to the Authorization Server to perform authentication and authorization. The user is displayed with the HTML page from the Authorization Server (phase 2).
3. The user has to input proper User Name. The Authorization Server gets the User Name and maps it into MSISDN, which is a format expected by OTA system in order to send push to the proper user’s device (phase 3).

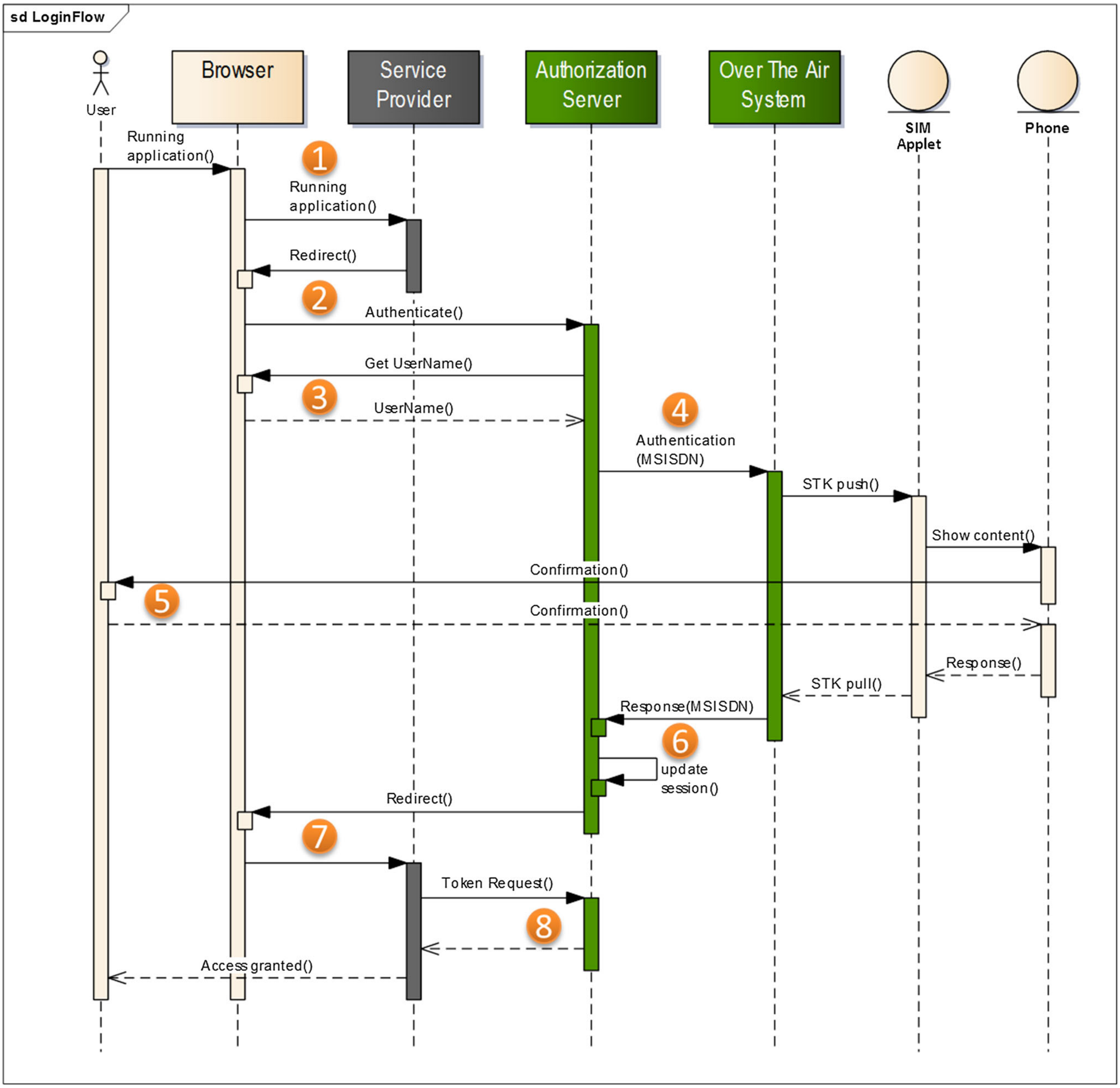


Fig. 2 Sequence diagram of the proposed authentication method

4. The Authorization Server sends request to OTA to authenticate the user. The OTA System sends reques to the applet on the SIM card, recognized by the MSISDN (phase 4).
5. Next, the applet on a SIM card responds to the command and displays the proper screen for the user's acceptance. The user is presented with a simple screen to decide whether to confirm his identity or to reject the request. Then the user confirms a willingness to log in to the service provider (phase 5).
6. After user's confirmation on the device, the SIM Applet responses to the OTA System. The OTA receives this information from the SIM Applet and sends a response to the Authorization Server with user's confirmation (phase 6).
7. The Authorization Server redirects the user back to the Service Provider by HTTP 302 Redirection. From the user perspective after clicking on the device there is an automatic redirection to the Service Provider web application via a web browser (phase 7).

8. Finally, Service Provider checks the user with the Token request according to the OpenID Connect standard. In order to do this the OTA sends a back-end request to the Authorization Server for the Token and user's information (phase 8).

In this paper the Authorization Server is deployed on a WebLogic server belonging to one of the Polish mobile operators, which is designed to be user-friendly, reliable and secure. We assume that the operating environment is secure. In this sense there is no malware. However, it is worth noting that there are no extra assumptions for the user authentication using this method, such as:

- There is no need for the user to install any mobile application on the mobile device,
- There is no application running in the background and waiting for notifications or requests.

In order to improve LoA, additional actions based on push STK may be implemented. The best solution that fits into this architecture is to implement a PIN (Personal Identification Number) entering instead of a single confirmation on the device. The PIN should be held only on the SE, not in any database. This way it is very secure, because the OTA system only requests the SIM card to verify the PIN, and then returns the information about the successful operation. No passwords are sent over the network. This way, if necessary, two or more factors authentication process can be created thereby increasing LoA. The objective of this paper, however, is to show the concept of creation of the authentication process based on the SIM card.

4 Details of the experimental methodology

For the proposed authentication method two types of user-oriented experimental evaluations were performed. The first is focused on establishing users' subjective perception of the proposed solution. In order to investigate overall users' awareness and attitude of usability, convenience and security towards different authentication processes the following experiment was designed. A questionnaire was prepared which allowed to determine the difference in users' perception for three different authentication approaches based on: static passwords, OTP (One-Time Password) SMS, and SIM card. The implementation of all three was based on OAuth 2.0 standard. All the evaluated methods are summarized briefly in Table 1.

The experimental methodology was as follows: a user was asked to use all three methods mentioned in Table 1 and successfully log in. The user has to log in to three web applications using Chrome browser on the laptop. Each web application required authentication in one of the three listed ways. For OTP SMS and SIM methods the users received a Samsung Galaxy A3 model number SM-A310F with a SIM card inside. The SIM card was able to receive the SMS and it had a proper applet installed on it. In case of failure in any method, the experiment for adequate authentication approach was repeated. After completing successfully these tasks, the user was asked to fill in a questionnaire.

Table 1 Investigated authentication methods

Method	Short description
Static password	User enters their login name and static password into the presented HTML form. After approval user is redirected to the page which he initially tried to log in. For the static password case no policy was recommended or enforced. Passwords have been set by users before conducting experiments
OTP SMS	User enters their login name into the HTML form. Then he receives the SMS with OTP and he has to copy this information into the form. After entering the correct OTP the user is redirected to the page which he initially tried to log in. OTP consisted of 6 characters, letters and numbers, with the exclusion of problematic characters such as o, i, 0 and 1
SIM	User enters his login name into the HTML form. Then he is asked for a confirmation on his smartphone by clicking Accept/Reject on the presented notification screen

The questionnaire was composed of 23 questions and its form is presented in the appendix. Each question was formulated in order to capture users' perception of the above-mentioned authentication methods from different angles. Furthermore, the same set of questions was asked for each method, which means that the user had to go through the same 23 questions three times. The respondents have been asked to answer each question by choosing one of the five proposed answers (so called 5-Likert scale [31]), which is usually used to determine participants' attitudes or feelings about something. This time it was used to measure the level of respondents' satisfaction or consent rate. Each participant had to choose one from the following answers:

1—Strongly disagree
2—Tend to disagree
3—No opinion
4—Tend to agree
5—Strongly agree

Table 2 Questionnaire utilized during experimental evaluation

Convenience	Using the proposed solution was frustrating	1
	Using this method was stressful	2
	I needed a lot of time to log in properly	19
	This method is prone to user's error	21
	Repeating the steps of this method may occur	22
Usefulness	This method meets my expectations	5
	The log in process was easy	6
	I felt that this method may be useful in everyday life	7
	I would be happy if I could use this method again	8
	This method was solid	9
	Using this method was quick	10
	This method requires improvements	12
	The method was user-friendly	13
	I liked using this method	14
	Using this method was convenient	17
Security	This method was trustworthy	11
	In my opinion this login method is safe	15
	The method seems to be easy to break	20
	It seems possible to impersonate someone else using this method	23
Difficulties	Logging in using this method was complicated	3
	While using this method I did not always know what to do next	4
	I needed additional instructions for using this method	16
	I had to focus hard while going through the log in process	18

All 23 questions were divided into four groups representing different aspects of the evaluated authentication methods: convenience, usefulness, security and difficulties. The appendix shows how the questionnaire looks like—there all the questions related to the similar topic have been rearranged in order to increase the reliability. These questions with the respective groups they represent, and the number in the correct order form the questionnaire are presented in Table 2.

The participants of the survey were balanced by age and gender. Forty respondents—thirty men and ten women—took part in the experiment with filling the questionnaire. The participants' age was between 20 and 50. Technical knowledge was highly diversified: from experts in the field of security to ordinary computer users. The participants represented various professional groups consisted of both students and IT employees as well as people completely unrelated to the IT industry, such as lawyers, pharmacists, builders, financiers or mechanics. Responders were explained the consecutive steps of the log in process without details related to the technical aspects of the methods.

Another aspect that was investigated is related to the time needed to conduct the whole log in process. The aim was to measure the time that a user needs to authenticate successfully. There was no point in measuring the log in time of the static password-based authentication. This is because this time would vary considerably depending on the complexity and length of the password (no security policy when setting the static password has been forced). This means that sometimes the duration of the whole process was really short, and if the participant chose a complex, more secure password then this time was obviously longer. That is why the time needed for each participant to log in has been measured only for OTP SMS and SIM methods.

For the purpose of these experiments the respondent has to put their login name (MSISDN) in the HTML form and confirm it by clicking the "Next" button, which is the moment the time measurement is initiated for both methods. Then, depending on the method, the participant sees another HTML form to put the OTP SMS or an HTML form with instructions to confirm the log in on the device. Copying the SMS OTP had to be approved by clicking on the HTML form. While confirming with SIM, the second HTML vanishes automatically. Typing in the correct OTP or confirming authentication with SIM resulted in redirecting the user to the Service Provider site, where the user tried to log in. The login time was calculated up to this point.

For experiments with SIM card-based authentication, 80 participants were asked to log in while the corresponding time was measured. It is also worth noting that for the OTP SMS-based authentication, the calculated log in duration has been performed on actual customers of one of the major mobile operators in Poland.

5 Results of the experimental evaluation concerning convenience

This chapter presents the results of research. We presented the results of the questionnaire survey and then the times of logins respectively.

5.1 Utility (questionnaire)

The sample of 40 respondents consisted of two groups of 20 participants. The groups were formed based on the respondents age, i.e. first group gathered participants of 25 years old

Table 3 Average scores of the obtained experimental results

	Static pass		OTP SMS		SIM	
Question	Average	SD	Average	SD	Average	SD
Using the proposed solution was frustrating	2.11	1.18	2.86	1.17	1.83	0.79
Using this method was stressful	2.06	1.35	2.26	1.12	1.71	0.79
I needed a lot of time to log in properly	1.97	1.25	2.91	1.14	1.69	0.61
This method is prone to user's error	4.17	2.34	3.66	1.33	2.00	0.99
Repeating the steps of this method may occur	4.00	1.13	3.97	0.96	2.77	0.82
This method meets my expectations	3.71	1.08	3.69	1.13	4.03	0.51
The login process was easy	3.94	1.17	3.71	0.92	4.51	0.82
I felt that this method may be useful in everyday life	3.54	1.06	3.54	1.11	4.17	0.85
I would be happy if I could use this method again	3.09	1.24	3.06	1.15	3.86	0.92
This method was solid	3.14	1.03	3.17	1.34	3.51	0.96
Using this method was quick	3.77	1.09	3.03	0.80	3.89	0.96
This method requires improvements	2.86	1.01	3.00	0.97	3.09	1.04
The method was user-friendly	3.29	1.25	3.03	1.18	4.46	0.56
I liked using this method	3.43	0.92	3.03	1.25	4.26	0.78
Using this method was convenient	3.69	1.18	2.91	1.06	4.43	1.07
This method was trustworthy	3.43	1.03	3.80	1.15	3.71	1.19
In my opinion this log in method is safe	3.20	1.05	3.63	1.04	3.17	0.61
The method seems to be easy to break	3.49	1.08	2.23	1.35	2.86	0.89
It seems possible to impersonate someone else using this method	4.00	1.07	3.20	1.34	3.37	0.83
Log in using this method was complicated	1.89	1.15	2.14	0.94	1.57	0.97
While using this method I did not always know what to do next	1.89	0.92	2.14	0.97	1.80	1.11
I needed additional instructions for using this method	1.63	1.08	2.03	0.75	2.06	1.14
I had to focus hard while going through the login process	1.89	1.11	2.31	1.16	1.74	1.19

or less, and the other group of more than 25 years. They were also balanced for gender, with 10 (25%) females. The experiment has been performed between July and December 2016. The average time taken to complete the questionnaire was about 20 minutes. All users have used the SIM card-based authentication for the first time, while the other methods were previously known.

The results have been divided into four following aspects of the investigated methods seen from the participants' perspective: difficulties, security, functionality and inconvenience. The mean individual attribute scores for the three investigated methods are shown in Table 3.

Starting from the "difficulties" group of questions, as expected, it turned out that the method with confirmation of identity by using the SIM card-based method was found the easiest one for participants. Respondents, while questioned directly about easiness of the method's usage, voted quite definitely in favor of the SIM card-based authentication as shown in Fig. 3. Surprisingly, despite the fact that this method was new for all participants, they considered it as the simplest one to use.

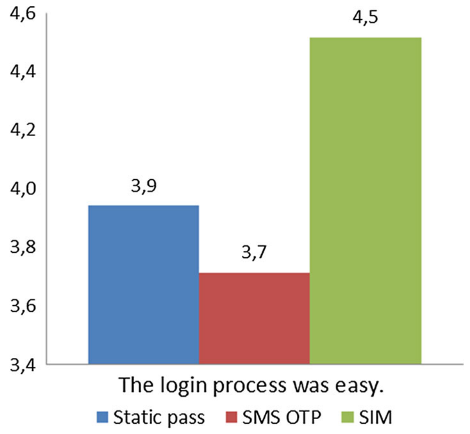


Fig. 3 Ease of use

In addition to the direct question about the ease of use of SIM card-based method, in the questionnaire there were also similar questions to determine the authentication simplicity. These questions were focused on the potential negative feelings that the participants could have toward this solution. The results are presented in Fig. 4. It has been found that the proposed method has been widely accepted by users. Interviewees indicated that they did not have to focus much on it and that the process was clearly the least complicated, even though it was new for them. It is widely believed that in general people fear novelty or newness as it typically involves some kind of change for them. However, by analysing the presented results we can conclude that the SIM-based method was very convenient and easy to use. Only one question related to instructions got negative response. The most likely explanation of this result is that respondents very often use the other methods and do not need any tips on how to use it. Because they had never used such type of authentication which relies on a single click only, they needed some guidance on what to do.

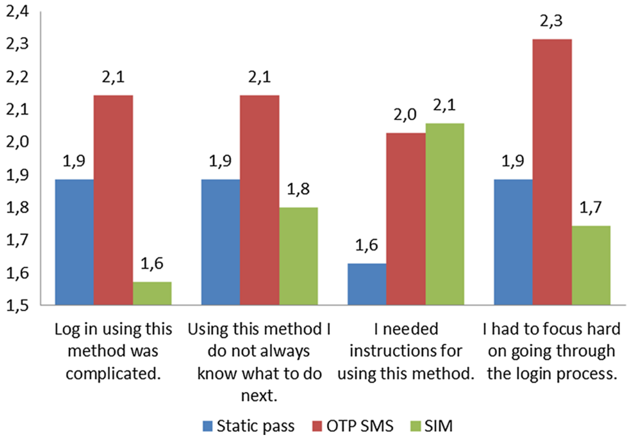


Fig. 4 Difficulties in use

Another set of nine questions concerned the usefulness of the authentication methods (Fig. 5). It can be easily seen that the method based on SIM card authentication yielded very good results. Respondents were keen to utilize this method in the future and consider it useful in their everyday life. This, in turn, means that they are more and more conscious about the issues associated with authentication in their everyday interaction with protocols/services and they would want to change it. Although the method was used by them for the first time, the participants described it as solid. Nevertheless, they could also see areas that could be improved. However, when it comes to questions about users' friendliness and convenience, it is the SIM-based method that gained the greatest appreciation among respondents. The results in this case showed a very significant difference in opinions. The issues related to the time of logging methods are pre-

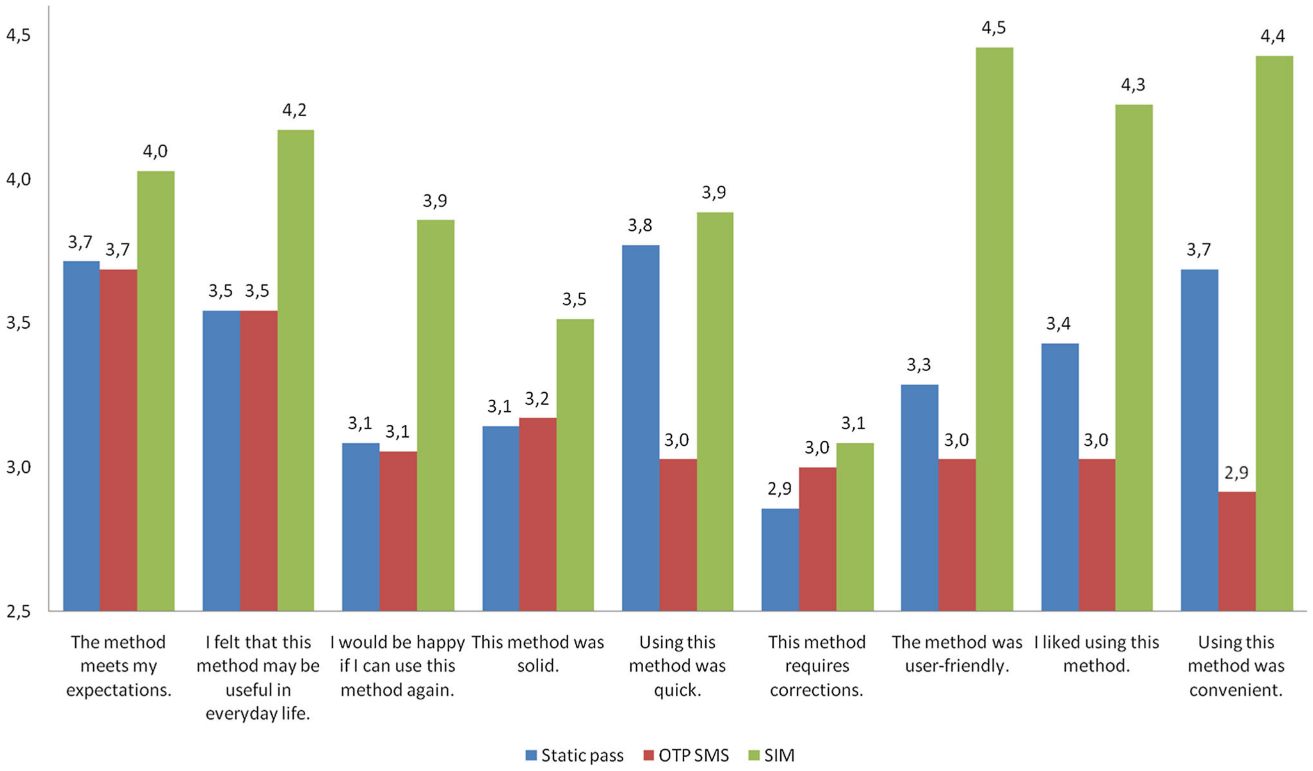


Fig. 5 Usability

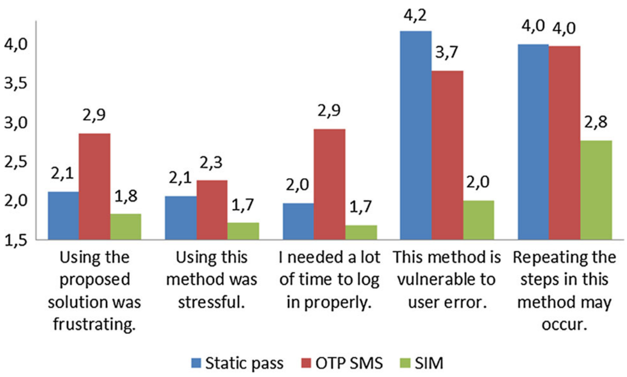


Fig. 6 Inconvenience

sented in the next section, but here, the results show that the static password-based method seems to be as fast as the SIM-based one. But it may also indicate the lack of security while using this method. It is our belief that the responders most probably had written down passwords which they use very frequently and know how to quickly type them into the login form. As mentioned earlier, due to the lack of any password policy during experiments, the password could have been of any length and complexity. Therefore, they were mostly short. For instance, it turned out that one of the participants used only one-character password.

The final study related to the questions that were supposed to measure the users' inconvenience is presented in Fig. 6. Based on the presented results it can be concluded that the participants find the SIM-based authentication in contrast to other methods, and think that it is harder to generate an error and repeating the steps in the log in process occurs less frequently. Errors in prescribing or entering passwords in the SIM-based method are totally eliminated. This confirms that this solution is convenient and simple to use. At the same time, the SIM-based authentication was selected by the participants as least stressful or frustrating. This confirms the positive impact the method has on its users.

The analysis and results of the questionnaire indicates that the authentication method based on SIM card could replace existing solutions, previously favored by users. One of the big advantages of this method is that it is easy and enjoyable to use. The next subsection proves that it is also fast.

5.2 Duration of the login process

A study was conducted to compare the login time for SIM-based and OTP-based methods. First, eighty participants, aged 25–50, have been asked to go through the whole log in process using the SIM-based method. For the SIM-based approach we captured the log in duration for 185 authentication instances.

Table 4 Duration of the log in operations for OTP and SIM-based methods

	SIM	OTP SMS
Number of log in operations	185	2198
Average time (s)	6.69	34.48
SD	5.28	31.78

For the OTP-based method participants of the experiment were recruited among customers of a mobile operator. In this case we were able to gather 2198 instances of successful log in operations.

Table 4 shows the results of the average duration of the log in operation for both authentication solutions. The experimental results match the expectation that the SIM-based method is really fast. The big difference when it comes to results for the OTP and SIM-based approaches comes from the fact that the user logs in with just one click. The complexity and length of the OTP would only decrease or increase the given difference.

6 Security analysis

This section presents the proposed method from the perspective of security. The previous sections have shown that the participants of the experiment, in general, like the SIM-based method. In this section, users' perception is described in terms of security (Sect. 6.1), and then a full security analysis of the new method has been made, in relation to network (Sect. 6.2) and mobile environment (Sect. 6.3). At the end of this section the well-known threats are presented along with a comparison of the authentication methods.

6.1 Users' perception

As it was mentioned above, it is commonly believed that people are typically afraid of novelties and innovations. Still, the results related to assessing the security of the method prove that it is not so obvious. Figure 7 shows that the SIM-based authentication does not deviate significantly from the other approaches. Quite on the contrary—it has never been pointed as the weakest solution. The security analysis has not been explained to responders before the experiments. The aim of this study was just to examine their general feelings and opinions. The results revealed that people do not have knowledge about authentication security solutions (which is not surprising). It is worth noting that there were contradictory answers about the OTP-based authentication: some respondents find it the most secure and later state that it is the easiest to break. Therefore, a more detailed analysis related to the security is presented in the next subsections.

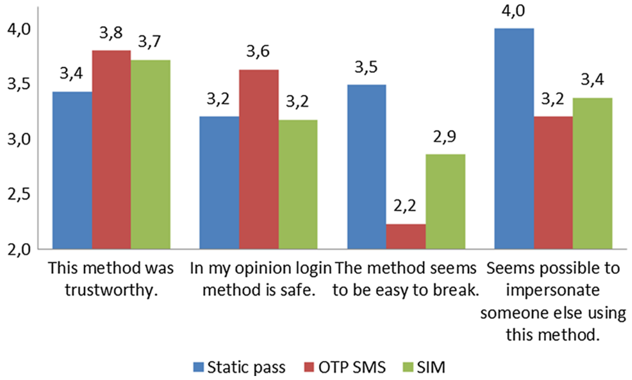


Fig. 7 Security

6.2 Network

First of all, it should be noticed that this solution uses a SSL/TLS. All traffic from the servers is encrypted.

In order to prevent cookies from being observed by unauthorized parties due to the transmission, the Authorization Server adds the secure flag while sending a new cookie to the user within an HTTP Response. As an additional flag, the HttpOnly flag is also included in a Set-Cookie HTTP response header, which helps mitigate the risk of client-side script accessing the protected cookie [32].

In addition to the application layer, at the Authorization Server the IP white lists are utilized. Only predefined IP addresses for both OTA server and Service providers servers are allowed. Moreover, the addresses of service providers are correlated with its IDs.

Furthermore, there is a time-counter started at the Authorization Server for the response from OTA. There is also a user lock after three failed attempts.

6.3 Mobile environments

When it comes to the mobile device, the SIM card communicates with the display differently depending on the operating system.

The STK requests are executed sequentially by layers: rild is responsible for direct contact with the SIM card TelephonyManager (CatService) and the application supports STK (usually com.android.stk). Newer versions of Android introduced a security feature that prevents operation of STK by any application while adding privilege RECEIVE_STK_COMMANDS.

In the iOS system applications cannot have a direct interaction with STK, which is operated by SimToolkitUI an extension of SpringBoard. The sandbox prevents applications from taking any actions in the system (usually applications are limited only to run in a specific, dedicated area), in particular to intercept STK messages.

When it comes to Windows Phone, the STK is supported by the SIM Toolkit service. Applications cannot make an interaction with other processes, particularly with SIM Toolkit service.

Performing jailbreak (iOS, Windows Phone) or root (Android) that allows STK messages interception is an expensive and technically complicated operation.

6.4 Threats

In addition, in the following part, we will investigate each method's resistance to many possible known attacks (Table 5).

A significant threat to the proposed authentication method seems to be the screen or keyboard sniffing. If the application is able to take administrator rights or gain enough permissions to capture messages intended for STK, it will be able to automatically authorize requests with the proposed method. That is why it is suggested to use multifactor authentication.

The additional threat to consider is an overlay attack. This attack permits an attacker to draw anything on top of any window and application running on the infected device. Once the attacker detects a STK push, the malware will redraw an exact login screen on top of the legitimate one or something completely new, into which the user clicks. Quite an effective method to defend against an overlay attack is to use personalized images or texts which the user can choose once and see every time when logging in. In case of screen overlay the user does not see their chosen image and, as a consequence, would not want to continue logging in.

Although the solution seems technically secure, it should be noticed that again the weakest link is a human user. Using the lowest LoA, it may happen that the user accidentally clicks and confirms their identity and thereby successfully finishes the authentication process. Therefore, for sensitive services it is recommended to use an additional authentication factor, such as PIN on SE.

7 Conclusion and future work

Authentication while using mobile device is an essential part of everyday life. In this paper the possibilities of using mobile devices such as mobile phones as a secure and very user-friendly way of confirming its user's identity were analyzed. Confirming the identity using a smartphone when trying to log in seems to be a very promising way for the future. That is why in this paper we proposed an innovative authentication scheme which relies on the Secure Element which is a SIM card. Performed experiments proved that the proposed authentication method can be very comfortable and user-friendly. In addition, it has been verified that this solution is extremely fast. Finally, potential security issues were

Table 5 Attacks and threats for all analyzed authentication methods

Threat/attack	Static password	OTP SMS	SIM
Man-in-the-middle	Possible between the browser and the Authorization Server	Possible between the browser and the Authorization Server, or between the device and SMSC	Possible between the browser and the Authorization Server, or between the device and OTA
Pass the hash	Probable	Only if password life time is long	Not possible
SQL or LDAP Injection	Probable	Not possible	Not possible
Cross-site scripting (XSS)	Probable. May be protected with HttpOnly flag	Probable. May be protected with HttpOnly flag	Probable. May be protected with HttpOnly flag
Brute force	Probable. There should be a limit of failed log in attempts	Probable. There should be a limit of failed attempts	Not possible
Dictionary attacks	Probable	Not possible	Not possible
User DDoS	Not possible	It may be that the user will be attacked with a huge number of SMS messages. There should be a limit of failed login attempts	It may be that the user will be attacked with a huge number of SMS messages. There should be a limit of failed login attempts
DDoS	It is possible to attack Authorization Server. There should be a firewall or a web application firewall installed	It is possible to attack Authorization Server or SMSC. There should be a firewall or a web application firewall installed	It is possible to attack Authorization Server or OTA. There should be a firewall or a web application firewall installed
Spoofing attack	Probable	Probable	Probable
Click-Jacking	Probable. May be protected with X-Frame-Options [33]	Probable. May be protected with X-Frame-Options [33]	Probable. May be protected with X-Frame-Options [33]
Hardware attack	There is no hardware to attack	Attack on the SIM card or the device. However, it is difficult to implement and requires the physical theft of the device	Attack on the SIM card or the device. However, it is difficult to implement and requires the physical theft of the device
Physical theft	Not possible	Probable. The device should be protected separately, for example, through a separate device PIN	Probable. The device should be protected separately, for example, through a separate device PIN

analyzed with conclusion that it is a secure authentication approach.

Future work includes completing the process with next authentication factors, which will rely on something the user knows, something the user has, and something the user is. In the future SIM cards will probably be replaced by eSIM, which would allow remote management of the applet.

Acknowledgements This research work was carried out thanks to a major mobile operator in Poland.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Appendix

	Investigated method (Static password, OTP SM or SIM)	1—Strongly disagree	2—Tend to disagree	3—No opinion	4—Tend to agree	5—Strongly agree
1	Using the proposed solution was frustrating					
2	Using this method was stressful					
3	Log in using this method was complicated					
4	While using this method I did not always know what to do next					
5	This method meets my expectations					
6	The login process was easy					
7	I felt that this method may be useful in everyday life					
8	I would be happy if I could use this method again					
9	This method was solid					
10	Using this method was quick					
11	This method was trustworthy					
12	This method requires improvements					
13	The method was user-friendly					
14	I liked using this method					
15	In my opinion this login method is safe					
16	I needed additional instructions for using this method					
17	Using this method was convenient					
18	I had to focus hard while going through the login process					
19	I needed a lot of time to log in properly					
20	The method seems to be easy to break					
21	This method is prone to user's error					
22	Repeating the steps of this method may occur					
23	It seems possible to impersonate someone else using this method					

References

1. https://www.statista.com. Statista [Online]. Available: https://www.statista.com/topics/2476/online-privacy/. Accessed February 5, 2017.
2. Kafle, V. P., Fukushima, Y., Fujikawa, K., & Harai, H. (2016). ID-based communication framework in future networks. *Wireless Personal Communications*, *86*(4), 1735–1750.
3. Thamizhchelvy, K., & Geetha, G. (2012). E-banking security: Mitigating online threats using message authentication image (MAI) algorithm. In *International conference on computing sciences (ICCS), 2012, Phagwara*.
4. Veeraraghavan, P., Almuairfi, S., & Chilamkurti, N. (2016). Anonymous paperless secure payment system using clouds. *The Journal of Supercomputing*, *72*(5), 1813–1824.
5. Kim, N. H., Lee, Y. S., Lim, H., Jo, H., & Lee, H. J. (2010). Online banking authentication system using mobile-OTP with QR-code. In *5th international conference on computer sciences and convergence information technology (ICCIT), 2010, Seoul*.
6. Fang, X., & Zhan, J. (2010). Online banking authentication using mobile phones. In *5th international conference on future information technology (FutureTech 2010), Busan*.
7. Kerttula, E. (2015). A novel federated strong mobile signature service—The finnish case. *Journal of Network and Computer Applications*, *56*, 101–114.
8. Fernandez-Saavedra, B., Sanchez-Reillo, R., Ros-Gomez, R., & Liu-Jimenez, J. (2016). Small fingerprint scanners used in mobile devices: The impact on biometric performance. *IET Biometrics*, *5*(1), 28–36.
9. Zareen, F. J., & Jabin, S. (2016). Authentic mobile-biometric signature verification system. *IET Biometrics*, *5*(1), 13–19.
10. Choi, H.-S., Lee, B., & Yoon, S. (2016). Biometric authentication using noisy electrocardiograms acquired by mobile sensors. *IEEE Access*, *4*, 1266–1273.
11. Liu, H., & Lazkani, E. E. (2016). Biometric inspired mobile network authentication and protocol validation. *Mobile Networks and Applications*, *21*(1), 130–138.
12. Ghouzali, S., Lafkih, M., Abdul, W., Mikram, M., El Haziti, Mohammed, & Aboutajdine, D. (2016). Trace attack against biometric mobile applications. *Mobile Information Systems*, *2016*, 1–15.
13. Torres, J., Izquierdo, A., & Sierra, J. M. (2007). Advances in network smart cards authentication. *Computer Networks*, *51*(9), 2249–2261.
14. Ashraf, M., Aziz, S. M., & Kabir, M. L. (2009). A SIM-based electronic transaction authentication system. *Computer Systems Science and Engineering*, *24*, 13–20.
15. Parka, H.-S., Leeb, H.-W., Leec, D. H., & Koa, H.-K. (2008). Multi-protocol authentication for SIP/SS7 mobile network. *Computer Communications*, *31*(11), 2755–2763.
16. Mishra, D., Das, A. K., & Mukhopadhyay, S. (2016). A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. *Peer-to-Peer Networking and Applications*, *9*(1), 171–192.
17. Islam, S. H., Obaidat, M. S., & Amin, R. (2016). An anonymous and provably secure authentication scheme for mobile user. *International Journal of Communication Systems*, *29*, 1529–1544.
18. Djellali, B., Belarbi, K., Chouarfia, A., & Lorenz, P. (2015). User authentication scheme preserving anonymity for ubiquitous devices. *Security and Communication Networks*, *8*(17), 3131–3141.
19. Gope, P., & Hwang, T. (2016). An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *Journal of Network and Computer Applications*, *62*, 1–8.
20. Tsai, J.-L., & Lo, N.-W. (2016). Provably secure anonymous authentication with batch verification for mobile roaming services. *Ad Hoc Networks*, *44*, 19–31.
21. Lu, Y., Li, L., Peng, H., & Yang, Y. (2016). Robust anonymous two-factor authenticated key exchange scheme for mobile client-server environment. *Security and Communication Networks*, *9*(11), 1331–1339.
22. Alizadeha, M., Abolfazlic, S., Zamanid, M., Baharunb, S., & Sakuraia, K. (2016). Authentication in mobile cloud computing: A survey. *Journal of Network and Computer Applications*, *61*, 59–80.
23. Yanga, X., Huanga, X., & Liu, J. K. (2016). Efficient handover authentication with user anonymity and untraceability for Mobile Cloud Computing. *Future Generation Computer Systems*, *62*, 190–195.
24. Mayrhofer, R. (2014). An architecture for secure mobile devices. *Security and Communication Networks*, *8*, 1958–1970.
25. Bicakcia, K., Unalb, D., Asciogluc, N., & Adalierc, O. (2014). Mobile authentication secure against man-in-the-middle attacks. *Procedia Computer Science*, *34*, 323–329.
26. Abid, M. H., Jan, F., Mustafa, T., & Faridi, M. S. (2012). Cloud computing: A general user's perceptions and security issues at Universities of Faisalabad, Pakistan. *International Journal of Computer Science Issues*, *9*(5), 375–380.
27. Weir, C. S., Douglas, G., Carruthers, M., & Jack, M. (2009). User perceptions of security, convenience and usability. *Computers and Security*, *28*(1–2), 47–62.
28. Sari, P. K., Ratnasari, G. S., & Prasetio, A. (2015). An evaluation of authentication methods for smartphone based on users' preferences. In *International conference on innovation in engineering and vocational education, Bandung*.
29. http://openid.net/ [Online]. Available: http://openid.net/specs/openid-connect-core-1_0.html. Accessed 2017.
30. Hardt, D. (2012). https://tools.ietf.org/html/rfc6749. Internet Engineering Task Force (IETF), October 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749. Accessed February 5, 2017.
31. http://www.simplypsychology.org [Online]. Available: http://www.simplypsychology.org/likert-scale.html. Accessed 2017.
32. https://www.owasp.org. OWASP [Online]. Available: https://www.owasp.org/index.php/HttpOnly. Accessed 2017.
33. https://www.owasp.org. OWASP [Online]. Available: https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet. Accessed 2017.

Pawel Laka is a Ph.D. student and holds M.Sc degree (2015) in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland. His rese arch interests include: multi-factor authentication and network security.

Wojciech Mazurczyk is an associate professor at the Institute of Telecommunications in the Faculty of Electronics and Information Technology at the Warsaw University of Technology, Poland and a researcher at the FernUniversitaet in Germany. His research interests include network security, information hiding, and network forensics. Mazurczyk received a Ph.D. and a D.Sc in telecommunications from the Warsaw University of Technology.