We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Multifactor Authentication Methods: A Framework for Their Comparison and Selection

Ignacio Velásquez, Angélica Caro and Alfonso Rodríguez

Abstract

There are multiple techniques for users to authenticate themselves in software applications, such as text passwords, smart cards, and biometrics. Two or more of these techniques can be combined to increase security, which is known as multifactor authentication. Systems commonly utilize authentication as part of their access control with the objective of protecting the information stored within them. However, the decision of what authentication technique to implement in a system is often taken by the software development team in charge of it. A poor decision during this step could lead to a fatal mistake in relation to security, creating the necessity for a method that systematizes this task. Thus, this book chapter presents a theoretical decision framework that tackles this issue by providing guidelines based on the evaluated application's characteristics and target context. These guidelines were defined through the application of an extensive action-research methodology in collaboration with experts from a multinational software development company.

Keywords: security, authentication scheme, multifactor authentication method, action-research, decision framework

1. Introduction

Generally, to protect the personal information of users in software applications, distinct authentication techniques are utilized to prevent intruders from accessing to it. Authentication is, thus, the process of verifying the identity of a user as part of a system's access control to protect the information stored within them [1]. Various authentication techniques have been proposed in literature, such as text passwords [2, 3], smart cards [4, 5], and biometrics [6–8]. All of the mentioned techniques belong to distinct authentication factors. An authentication factor is a piece of information that can be used to verify the identity of a user [9]. There are three main groups or factors of authentication techniques [10, 11]: (i) knowledge-based, that is, based on something that the user knows, such as text passwords; (ii) possession-based, that is, based on something that the user possesses, such as smart cards; and (iii) inherence-based, that is, something that the user is, such as biometrics. Two or more of these techniques can be combined to increase security, which is known as multifactor authentication [1].

In this book chapter, to differentiate between single-factor and multifactor authentication techniques, the former will be referred to as **authentication schemes**, whereas the latter will be referred to as **multifactor authentication methods**.

Nowadays, the decision of what authentication scheme or method to implement in a software application resides within the software development team. However, the experience of the involved developers can vary from team to team, which could affect in the decision of what authentication technique to implement. Due to the importance of security [12], selecting the wrong authentication technique could potentially be a fatal mistake [13].

The above statement creates the necessity of a method that systematizes the task of comparing and selecting the authentication schemes and methods. A few frameworks in literature partially help to achieve this [14, 15]; however, they do not present the adequate characteristics for their application in distinct application contexts or do not consider all authentication techniques or multifactor authentication. Thus, this book chapter presents a decision framework that covers the observed gap. This framework has been generated through the application of an action-research methodology [16]. This action-research has been performed in collaboration with a multinational software development company and contemplates the utilization of other research methodologies that support it.

The remainder of this book chapter is organized as follows. The methodology utilized for the research is presented in Section 2. Section 3 is focused on obtaining of the knowledge base utilized for the research. In Section 4, the generated decision framework is presented. Section 5 consists on the validation of the framework. Finally, the conclusions and future work of the research are given in Section 6.

2. Methodology

The realization of this research is within the scope of an action-research methodology that was carried for over a year in collaboration with a software development company. The objective of action-research is to provide a benefit for the research's "client" while also generating relevant "research knowledge" [16, 17]. This kind of collaboration allows to study complex social processes, such as the use of information technologies in organizations, by introducing changes in them and observing their effects [18].

There are four roles involved in action-research [19]. These roles are as follows:

- The **researcher(s)** who undertake(s) the action-research. In this case, the researchers are the book chapter's authors.

- The **studied object**, that is, the problem to solve. In this case, the studied object is the comparison and selection of authentication schemes and methods.

- The **critical group of reference** that has a problem that needs to be solved and also participates in the research process. In this case, the critical group of reference is composed by the employees of the partnered software development company (PSDC).

- The **beneficiary** who can receive benefits from the research results, without directly participating in its process. In this case, the main beneficiary is the PSDC, but other software developers can also benefit from this research.

During the realization of this action-research, multiple activities were performed in conjunction with the PSDC. These activities helped to generate and validate the proposed decision framework for solving the need of automatizing the comparison and selection of authentication techniques. These activities were performed utilizing the iterative process of action-research, which considers, for every cycle, the following four phases [20]: (i) the planning phase, which considers the elaboration of a research question to be answered through the iteration; (ii) the action phase, where distinct research methodologies are applied to address the posed research question; (iii) the observation phase, where the results of the interventions from the previous phase are processed; and (iv) the reflection phase, where the researchers shares their finding with the group of reference to generate feedback; it is also possible to transversely perform this phase instead of cyclically [19], as it was done in this action-research through the realization of weekly progress meetings.

In this work, the action-research methodology was applied through three cycles. The objective of the first cycle was to obtain the required knowledge base for creating the framework. To achieve this, two strategies were applied: first, a systematic literature review (SLR) [21] was performed to obtain the existing knowledge in literature, and secondly, a number of surveys and interviews [16, 22] were conducted to learn the perceptions of the industry through the PSDC's employees. The second cycle was centered on the creation of the decision framework. During this cycle, an expert panel [23] was held to validate the initial draft of the framework. Finally, the third cycle focused on validating the final framework through the application of case studies [24].

3. Identification of the knowledge base

To construct the decision framework, it was necessary to obtain an adequate knowledge base regarding the topic at hand. To achieve this, two methodologies were applied. The first was the realization of a systematic literature review to identify the existing knowledge in related academic publications. The second corresponds to the application of a survey and interviews (S&I) to employees of the PSDC to learn the perceptions of the industry. The combined usage of these methods allowed the procurement of a knowledge base useful both for the academic and industrial sectors.

3.1 Systematic literature review

A systematic literature review has been carried out with the objective of "identifying authentication schemes proposed in literature and their possible combinations for their use as multifactor authentication methods, while also detecting criteria used for their comparison and selection and the existence of frameworks that handle such a task." Based on this objective, the following four research questions were formulated:

1. Which are the main authentication schemes that exist in the literature?

2. What combinations of these schemes can be found that can be used as multifactor authentication methods?

3. What criteria can be used to compare and/or to select between authentication schemes and/or multifactor authentication methods?

4. Are there frameworks that help to compare and/or to select authentication schemes or multifactor authentication methods? What are their characteristics?

The planning and results of the SLR have already been published in literature [25]. Additionally, a list containing the publications accepted during the SLR can be found in http://colvin.chillan.ubiobio.cl/mcaro/. Next, a brief summary of the main results of the SLR for every research question is presented.

3.1.1 Authentication schemes

A total of 515 publications regarding the proposal of authentication schemes were found. Their distribution among the authentication factors is as shown in **Figure 1**. Additionally, the context for which these schemes were proposed was recorded as well; this is presented in **Table 1**, including the publication's origin (journal article, conference article, or book chapter). It is important to mention that only 233 of the publications indicated a context.

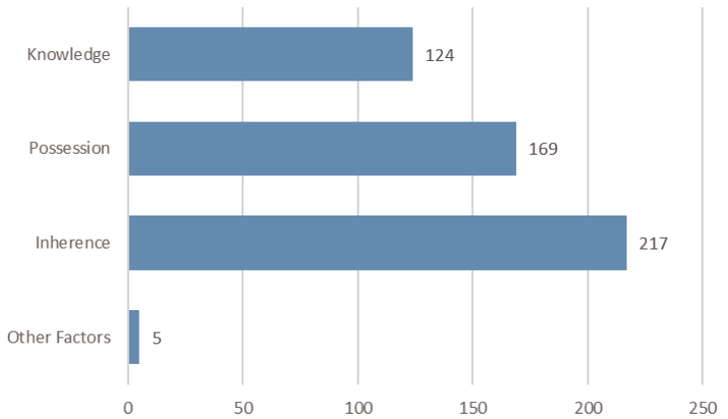


Figure 1.
Number of publications proposing authentication schemes for every authentication factor.

Context	Journal	Conference	Book	Total
Mobile environment	38	43	0	81
Remote authentication	31	11	0	42
Healthcare/telecare	23	1	0	24
Multi-server environment	15	2	0	17
Continuous authentication	9	2	0	11
Wireless sensor networks	8	2	0	10
Cloud computing	3	4	2	9
Banking and commerce	2	6	0	8
Smart environment	2	5	0	7
Login protocols	5	0	0	5
Web applications	4	1	0	5
Other contexts	7	7	0	14
Total	147	84	2	233

Table 1.
Number of publications proposing authentication schemes for every context.

3.1.2 Multifactor authentication methods

Four hundred forty-two publications proposing the combination of two or more authentication schemes in a multifactor manner were identified. Their distribution among the distinct authentication factor combinations is as shown in **Figure 2**. Similarly to the previous research question, the context for which these methods were proposed was recorded as well; this is presented in **Table 2**, including the publication's origin (journal article, conference article, or book chapter). In this case, 272 of the publications did indicate a context.

3.1.3 Comparison and selection criteria

Only 17 publications presented criteria for the comparison and selection of authentication schemes and methods. The presented criteria in the distinct publications can be categorized based on the kind of criteria proposed. Every publication

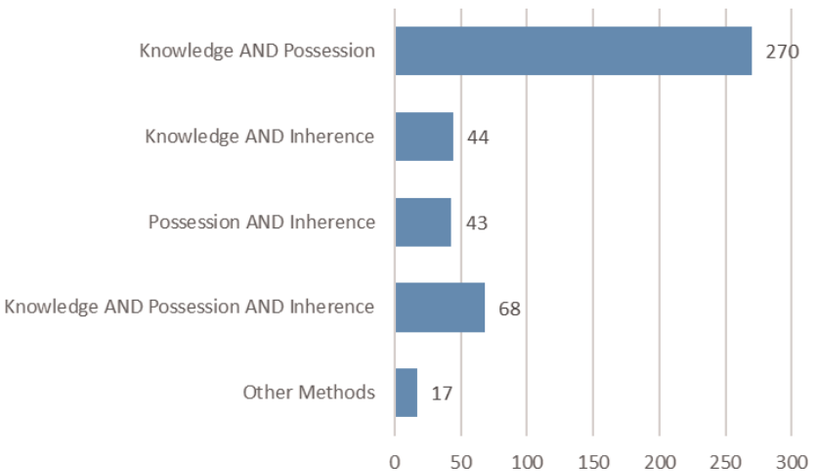


Figure 2.
Publications proposing authentication methods for every factor combination.

Context	Journal	Conference	Book	Total
Remote authentication	52	12	0	64
Healthcare/telecare	45	3	0	48
Wireless sensor networks	29	4	0	33
Multi-server environment	22	7	0	29
Mobile environment	10	11	0	21
Cloud computing	12	5	0	17
Banking and commerce	6	5	0	11
Web applications	5	6	0	11
Wireless networks	6	2	0	8
USB devices	1	5	0	6
Insecure environment	3	2	0	5
Other contexts	15	3	1	19
Total	206	65	1	272

Table 2.
Number of publications proposing authentication methods for every context.

considered one or more criteria categories; however, only three of them could be identified in more than one publication. The most identified categories of criteria are usability, security, and costs. The first two were identified in nine publications each, whereas the latter was found in five publications.

Moreover, it could be observed that most of these articles highly considered the importance of the use context for comparing and selecting schemes and methods. This was mainly done by the publication addressing specific contexts or considering the context itself as another criterion.

3.1.4 Decision frameworks

Eight decision frameworks that help in the comparison and selection of authentication schemes and methods were identified. Through the analysis of these frameworks, it could be observed that multifactor authentication is not often considered, whereas proposals that do consider it utilize a limited number of criteria. Thus, no decision framework that considered multifactor authentication and enough criteria for a detailed comparison and selection of authentication schemes and methods could be found.

3.2 Survey and interviews

A survey and interviews have been applied to the PSDC's employees with the objective of learning the perceptions of people from the industry regarding authentication and the comparison and selection of distinct schemes and methods. The interviews were realized as a pilot application of the survey. A total of 12 employees were interviewed. In addition, 45 valid responses, out of a sample of 83 people ranging from developers to project leads, were received through the survey. Out of the 57 respondents, over two thirds of them held a senior position in the PSDC, as well as having over 6 years of working experience.

Four main questions were posed to the respondents, whose contents can be summarized as follows:

Q1. What authentication schemes do you know?

Q2. What multifactor authentication methods do you know?

Q3. What authentication schemes or multifactor authentication methods have you implemented in applications that you have developed?

Q4. What is the importance that you give to distinct factors when deciding what authentication scheme or method should be implemented in an application?

In http://colvin.chillan.ubiobio.cl/mcaro/ it is possible to find the questionnaire used for the survey. A summary of the responses obtained for every question is provided next.

3.2.1 Authentication schemes known by the respondents

For this question, respondents were asked to mark from a list the authentication schemes that they knew. The most known schemes were text passwords, one-time passwords (OTP, tokens), and mobile-based authentication. All respondents answered this question. The complete results of this question can be observed in **Table 3**, which shows the number of survey respondents and interviewed people that know each authentication scheme.

Authentication scheme	Interviewees	Survey respondents
Text passwords (TP)	10	40
Graphical passwords (GP)	1	20
Cognitive authentication (CA)	0	10
OTP (tokens)	7	38
Smart cards (SC)	3	24
Mobile-based (MB)	8	31
Biometrics (B)	5	30
Federated single sign-on (FSSO)	4	22
Proxy-based (PB)	1	8
Others	0	2

Table 3.
Number of respondents that know each authentication scheme.

3.2.2 Multifactor authentication methods known by the respondents

For the second question, respondents were given a brief explanation about multifactor authentication. Afterward, they were asked what multifactor authentication methods they knew. The combination of text passwords and OTP was the most known among them. A total of 27 out of the 45 survey respondents answered this question. The complete results of this question can be observed in **Table 4**, which shows the number of survey respondents and interviewed people that know each multifactor authentication method.

Combination	Method	Interviewees	Survey respondents
Knowledge + possession	TP + OTP	7	15
	TP + SC	2	8
	TP + MB	6	6
	Others	0	1
	Total	15	30
Knowledge + inherence	TP + B	0	15
	Others	0	3
	Total	0	18
Possession + inherence	OTP + B	0	6
	MB + B	0	3
	SC + B	0	3
	Total	0	12
Knowledge + possession + inherence	TP + SC + B	0	7
	TP + OTP + B	1	2
	Others	0	2
	Total	1	11
Grand total		16	71

Table 4.
Number of respondents that know each authentication method.

3.2.3 Authentication schemes and methods implemented by the respondents

Next, the respondents were asked what authentication techniques they had implemented in applications developed by them and the kind of application. Most applications were either web-based or for banking and commerce. A total of 23 out of the 45 survey respondents answered this question. The complete results of this question can be observed in the graphs of **Figures 3** and **4**, which show the implemented authentication schemes and methods and the contexts of the applications that were being developed, respectively.

3.2.4 Comparison and selection criteria used by the respondents

For the last question of the S&I, distinct strategies were applied between the interviewees and the survey respondents. In the case of the former, they were directly asked what criteria they utilized for the comparison and selection of authentication schemes and methods. In the case of the latter, the responses from the interviewees, coupled with the results of the previously performed SLR, were used to generate a list of comparison and selection criteria that respondents were asked to value from 1 to 5. A higher value meant that the respondent gave a higher importance to the criterion. A total of 29 out of the 45 survey respondents answered this question. The complete results of this question can be observed in **Table 5** and

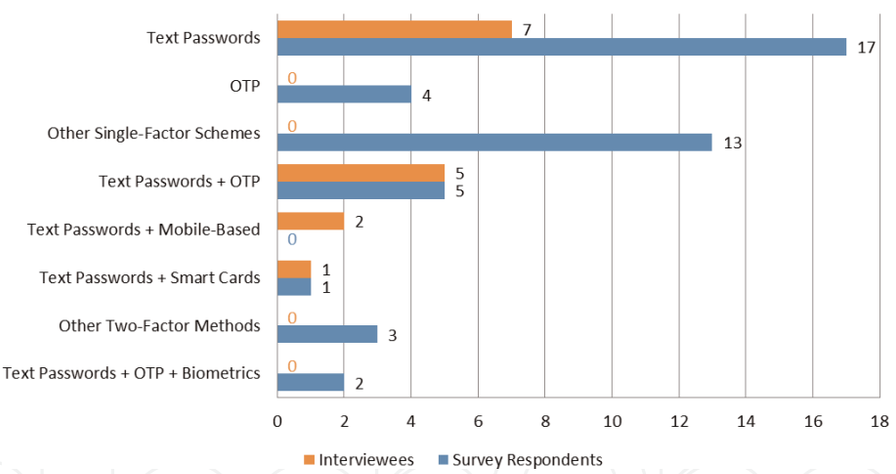


Figure 3.
Authentication schemes and methods implemented by the respondents.

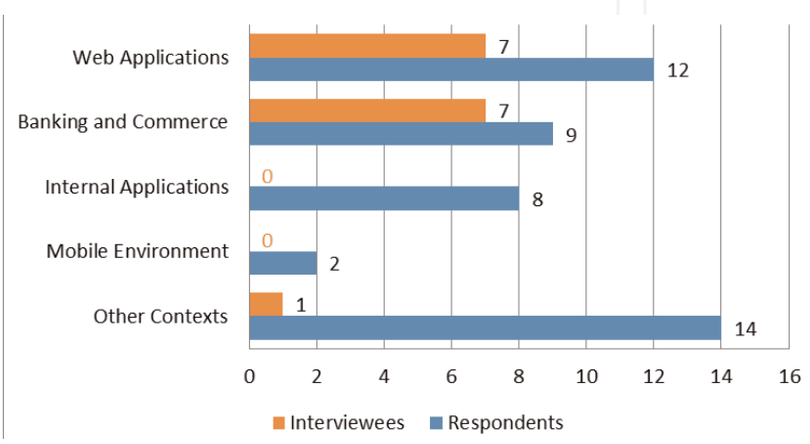


Figure 4.
Contexts of the applications developed by the respondents.

Criterion	Interviewees that consider the criterion
Client's requirements	11
Application context	11
Usability-related criteria	9
Security-related criteria	11
Cost-related criteria	8
Other criteria	2

Table 5.
Comparison and selection criteria considered by the interviewees.

in **Table 6**, which show the responses given by the interviewees and the survey respondents, respectively.

Finally, survey respondents were asked what other comparison and selection criteria they would consider. The received answers include the ease of authentication information recovery, the registration method, and the sensitivity of the information.

3.3 Short survey

A second survey was later applied to nine employees of the PSDC. These employees were selected among the most experienced developers of the company, based on their years of experience and positions. The single aim of this survey was to ascertain the importance that the respondents would assign to an application's security and usability based on the target context. The importance was valued in percentages, with the sum of usability and security being 100% for every context. **Table 7** presents the results of this survey.

The obtained values were used afterward as part of the input for the decision framework.

Category	Criterion	Value
Usability	Ease of use	3.31
	Ease of learning	3.28
	Need of using a device	3.10
	Method's reliability	4.10
Security	Importance of security	4.41
	Resistance to well-known attacks	4.21
Costs	Implementation costs	4.07
	Costs per user	4.00
	Server compatibility	3.69
	Need of acquiring licenses	3.86
	Available technologies	3.93
Others	Client's requirements	4.17
	Application context	4.41
	Norms and legislation	3.90

Table 6.
Comparison and selection criteria valued by the survey respondents.

Context	Importance of security (%)	Importance of usability (%)
Mobile environment	45.56	54.44
Remote authentication, multi-server environment, cloud computing	64.44	35.56
Healthcare/telecare	57.78	42.22
Wireless sensor networks	63.33	36.67
Banking and commerce	73.33	26.67
Web applications	28.89	71.11

Table 7.
Importance given to security and usability in distinct contexts by the respondents.

4. The framework

This section describes the decision framework constructed through the knowledge base acquired by using the methodologies presented above. It has been given the name of Kontun framework, which means "to enter foreign property" in Mapudungún, an indigenous language from Chile, which is what it aims to prevent. **Table 8** shows a summary of the main findings during the knowledge base gathering and their origin (either the SLR or the S&I).

A summary of the constructed framework's characteristics is provided next. A complete description can be found in [26].

First, the framework considers a number of criteria obtained from the knowledge base, divided among the three most observed categories: security, usability, and costs. Each criterion is then given distinct possible importance values and a weight based on the findings from the knowledge base. To illustrate the above

Most reported knowledge-based schemes	• Text passwords (SLR, S&I) • Graphical passwords (SLR)
Most reported possession-based schemes	• Smart cards (SLR) • OTP (S&I) • Mobile-based (S&I)
Most reported inherence-based schemes	• Face biometrics (SLR, S&I) • Behavioral biometrics (SLR) • Palm print (SLR) • Fingerprints (SLR, S&I) • Vein biometrics (SLR) • Iris biometrics (SLR, S&I)
Multifactor authentication	• Prevalence of the combination of knowledge- and possession-based authentication schemes (SLR, S&I)
Most observed application contexts	• Mobile environment (SLR) • Remote authentication (SLR) • Multi-server environment (SLR) • Cloud computing (SLR) • Healthcare/telecare (SLR) • Wireless sensor networks (SLR) • Banking and commerce (S&I) • Web applications (S&I)
Comparison and selection criteria	• Criteria are mainly related to usability, security, and costs (SLR) • Identified criteria are valued positively by the industry (S&I) • High importance observed regarding application context (SLR, S&I)

Table 8.
Summary of the acquired knowledge base.

criterion, **Table 9** shows the usability-related criteria, their importance values, and their weights.

Every criterion has two or more importance values between 20 and 100, and the sum of all the weights of the criteria belonging to the same category is 100%. In this manner, when using the framework, a person must select the importance values that best describe their application and then calculate the average values of security (S), usability (U), and costs (C) using the following equations:

$$S = \sum_{\text{for each criterion of } S} AssessmentValue * CriterionWeight \quad (1)$$

$$U = \sum_{\text{for each criterion of } U} AssessmentValue * CriterionWeight \quad (2)$$

$$C = \sum_{\text{for each criterion of } C} AssessmentValue * CriterionWeight \quad (3)$$

The framework also considers a number of common contexts identified through the knowledge base. These contexts were given distinct weights based on the importance of security and usability in the context itself. Here, a term known as the security/usability value (SUV) is presented. The knowledge base allowed to ascertain the fact that, generally, the more secure an authentication scheme or method is, it has a lower usability and vice-versa. The SUV is used to denotate this. Based on the calculated average values of S, U, and C, coupled with the selected application context (Ct), the SUV is calculated as follows:

$$SUV = A * S + B * (100 - U) \quad (4)$$

A and B are constants defined based on the importance given to S and U, respectively, in the selected context. A high SUV value thus indicates that more

Criterion	Importance	Value	Weight
Ease of use	The method necessarily needs to be easy to use	100	25%
	The method preferably needs to be easy to use	60	
	It is not necessary for the method to be easy to use	20	
Ease of learning	A user should not take longer than a day to get used	100	25%
	A user should not take longer than a week to get used	60	
	The time it takes to get used is not relevant	20	
Authentication information recovery	The recovery process should be simple	100	10%
	The recovery process should be complex	20	
Need of using a device	It does not need to use a device	100	10%
	It can use a possession or biometric device	60	
	It can use both a possession and a biometric device	20	
Authentication method's reliability	It should never or hardly fail during authentication	100	30%
	It should not fail occasionally during authentication	75	
	It can fail occasionally during authentication	45	
	It does not matter how often it fails	20	

Table 9.
Criteria considered by the framework.

secure authentication methods should be implemented in the application, whereas a low SUV indicates that more usable authentication schemes or methods should be implemented in the application.

Having calculated the SUV and also considering the average value given to C, the framework is able to provide a suggestion on what authentication schemes or methods to implement in the evaluated application. The recommendation is as follows: for a SUV of 65 or higher, the framework will suggest the implementation of highly secure authentication methods; for a SUV of 35 or lower, the framework will suggest the implementation of highly usable authentication schemes; and for a SUV between 35 and 65, the framework will suggest the implementation of averagely secure and usable authentication methods. Moreover, for a value of C of 60 and above, the framework will suggest the implementation of more affordable authentication schemes or methods; for a value of C below 60, the framework will suggest the implementation of more expensive authentication schemes or methods. The recommendations are also different based on the target Ct. Thus, for every Ct, the framework will give six possible recommendations based on the calculated SUV and C. **Table 10** illustrates the above framework for the context of mobile environment.

Finally, the person utilizing the framework must decide the authentication scheme or method to implement in their application, taking into consideration the recommendations given by the framework.

4.1 Tool prototype

To facilitate the use of the framework in software development environments, a tool prototype has been constructed that allows its utilization in a semiautomatic manner. This tool has also supported the validation process of the framework. With the tool prototype, the person in charge only needs to indicate the evaluated application's features and target context through a radio form. Afterward, the tool prototype automatically calculates the values of average S, U, and C and the SUV. The tool prototype is available for download in http://colvin.chillan.ubiobio.cl/mcaro/.

$SUV \geq 65$ $C < 60$	Graphical passwords + smart cards + behavioral biometrics Text passwords + OTP + behavioral biometrics Graphical passwords + OTP + behavioral biometrics Graphical passwords + OTP + face biometrics
$SUV \geq 65$ $C \geq 60$	Text passwords + smart cards + behavioral biometrics Text passwords + smart cards + face biometrics
$35 < SUV < 65$ $C < 60$	Graphical passwords + behavioral biometrics OTP + behavioral biometrics Text passwords + palm print/fingerprints Graphical passwords + OTP
$35 < SUV < 65$ $C \geq 60$	Text passwords + behavioral biometrics Text passwords + smart cards
$SUV \leq 35$ $C < 60$	Behavioral biometrics Graphical passwords Face biometrics Palm print/fingerprints
$SUV \leq 35$ $C \geq 60$	Behavioral biometrics Text passwords Graphical passwords

Table 10.
Recommendation given by the framework for the context of mobile environment.

The tool prototype has been developed using the model view controller (MVC) design pattern, with the Java programming language and supported by the Spring Framework. PostgreSQL has been used as the database management system.

The main screens of the tool prototype can be observed in **Figures 5–7**. They show the procedures for the criteria selection, the context selection, and the framework's recommendation, respectively.

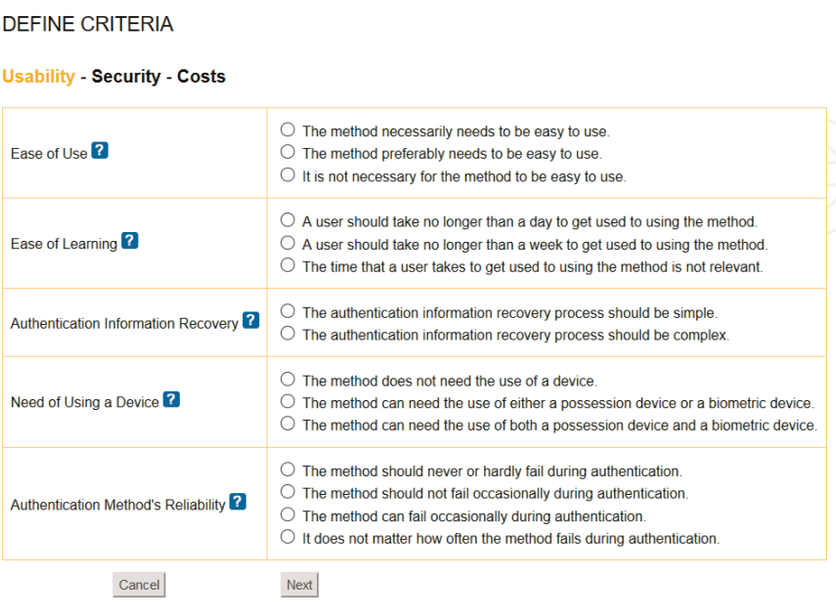


Figure 5.
Criteria selection in the tool prototype.



Figure 6.
Context selection in the tool prototype.

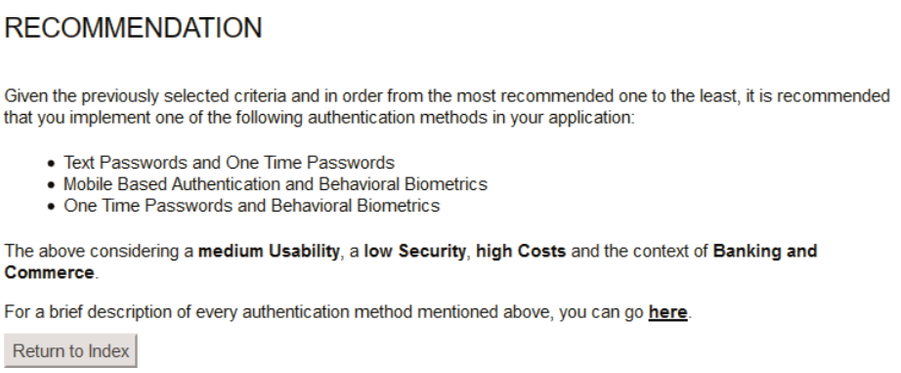


Figure 7.
Framework's recommendation in the tool prototype.

The tool prototype also has additional features that facilitate its use in software development companies. Specifically, it has a user registration feature which allows maintaining a registry of its usage and a functionality for adapting its preferences based on the software development company's needs.

5. Validation through the industry

Through the creation of the framework, its adequacy was repeatedly validated using strategies associated to the application of the action-research methodology. Specifically, the validation was ascertained through the realization of an expert panel and the application of case studies. These are detailed in remainder of this section.

5.1 Expert panel

An expert panel was held in collaboration with five experts from the PSDC that consisted of four sessions with the aim of ascertaining their perceptions regarding an initial draft of the framework, so that it was more adequate to the real requirements observed in a software development environment. The activities during every session of the expert panel are described next.

5.1.1 Presentation of the initial draft of the framework

The first session consisted on the presentation of the initial draft of the framework, with the purpose of helping the experts to have a general notion of the aim of this research.

5.1.2 Validation of comparison and selection criteria

The preliminary list of criteria, their categorization, their values, and their weights were presented to the experts for their validation. This allowed to discard the least adequate ones and to generalize those that were too specific for the needs of a software development team.

5.1.3 Validation of the considered contexts

The contexts considered by the framework were presented to the experts. Similarly to the previous session, this allowed to make the appropriate modifications to the currently selected contexts. Additionally, the SUV was presented to the experts, who generally agreed to the adequacy of its use.

5.1.4 Validation of the framework's recommendations

The authentication schemes and methods recommended for every situation were presented to the experts. This allowed to ascertain the adequacy of every recommendation. The experts were generally in agreement with the recommendations.

5.2 Case studies

After its construction, the validation of the framework's recommendations was realized through the application of a case study methodology in collaboration with

the PSDC. Specifically, the framework's recommendations were compared with the authentication schemes or methods implemented in existing applications developed by the PSDC or with the recommendations that their experts would give for hypothetical situations. The case studies are described in detail in [26]. Next, a brief summary of their application is provided.

The case studies are split in three categories: (i) those that were realized by comparing the framework's recommendation against the implemented scheme or method on an existing application, (ii) those that were realized by comparing the framework's recommendation against the recommendations given by experts for hypothetical applications, and (iii) those that were realized by comparing the framework's recommendation against the implemented scheme or method on an existing application and also against the recommendation given by experts for hypothetical applications with nearly the same features as the existing ones. These case studies are presented in **Tables 11–13**, respectively, presenting the implemented scheme or method in the existing application, the framework's recommendation, the most recommended scheme or method by the experts, and the acceptance rate of the framework's recommendation, as appropriate.

In general, the results of the case studies are favorable for the framework. It is important to mention that, where discrepancies are observed, there was often a reasoning behind them. For example, for case study 3 (existing application), the implemented scheme was demanded by the client and not selected by the software development team.

ID	Implemented scheme or method	Framework's recommendation
1	Two-factor authentication (text passwords + smart cards)	Three-factor authentication (text passwords + OTP + behavioral biometrics)
2	Two-factor authentication (text passwords + mobile-based)	Two-factor authentication (text passwords + mobile-based)
3	OTP (demanded by client)	Behavioral biometrics

Table 11.
Case studies based on existing applications.

ID	Experts' recommendation	Framework's recommendation	Acceptance rate of framework's recommendation
4	Two- or three-factor authentication	Three-factor authentication	100%
5	Text passwords	Two-factor authentication	80%

Table 12.
Case studies based on hypothetical applications.

ID	Implemented scheme or method	Experts' recommendation	Framework's recommendation	Acceptance rate of framework's recommendation
6	Two-factor authentication	Text passwords	Text passwords	100%
7	Text passwords	Two-factor authentication	Two-factor authentication	90%

Table 13.
Case studies based on existing applications with a hypothetical counterpart.

6. Conclusions

The research presented in this book chapter summarizes the definition of a theoretical framework. This framework will help in the comparison and selection of the most appropriate authentication schemes or multifactor authentication methods for applications created by software developers. It has been created through the application of an action-research methodology that considered the utilization of various other research methodologies that helped to contribute in distinct ways to the research objective.

On the one hand, a systematic literature review, coupled with surveys and interviews, was performed to obtain the required knowledge base for generating the framework. The utilization of these two methodologies allowed to ascertain the perceptions on authentication from both the academy and the industry.

On the other hand, an expert panel and several case studies were realized to validate the adequacy of the framework. This permitted to obtain feedback from the end users of the framework so that it would provide adequate authentication scheme or method recommendations and have an appropriate usability.

Thus, this experience allowed to observe the usefulness of performing a research in collaboration with the industry, as it permits obtaining results that align more adequately with their needs while also providing more refined academic results.

Several future work lines can be followed based on this research. Namely, the framework could be adapted to work as a recommendation system so that its recommendations get refined through its usage. For the industry, it would be of interest that the framework not only recommends an authentication technique but that it also provides the required code for its implementation. Finally, the last cycle of the action-research, that is, the realization of case studies, could be replicated in other software development companies to further validate the adequacy of the framework.

Acknowledgements

This research is part of the following projects: DIUBB 144319 2/R and BuPERG (DIUBB 152419 G/EF).

Author details

Ignacio Velásquez, Angélica Caro* and Alfonso Rodríguez
Computer Science and Information Technologies Department, University of Bío-Bío, Chillán, Chile

*Address all correspondence to: mcaro@ubiobio.cl

IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] O'Gorman L. Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE. 2003;**91**(12):2021-2040

[2] Kumari S, Khan MK, Li X, Wu F. Design of a user anonymous password authentication scheme without smart card. International Journal of Communication Systems. 2016;**29**(3): 441-458

[3] Ranjan P, Om H. An efficient remote user password authentication scheme based on Rabin's cryptosystem. Wireless Personal Communications. 2016:1-28

[4] Yang TC, Lo NW, Liaw HT, Wu WC. A secure smart card authentication and authorization framework using in multimedia cloud. Multimedia Tools and Applications. 2017;**76**(9):11715-11737

[5] Mishra D, Das AK, Mukhopadhyay S. A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. Peer-to-Peer Networking and Applications. 2016;**9**(1):171-192

[6] Samangouei P, Patel VM, Chellappa R. Facial attributes for active authentication on mobile devices. Image and Vision Computing. 2017;**58**:181-192

[7] Antal M, Szabó LZ. Biometric authentication based on touchscreen swipe patterns. Procedia Technology. 2016;**22**:862-869

[8] Usha K, Ezhilarasan M. Robust personal authentication using finger knuckle geometric and texture features. Ain Shams Engineering Journal. 2016;**9**(4):549-565

[9] Jacomme C, Kremer S, editors. An extensive formal analysis of multi-factor authentication protocols. In: 2018 IEEE 31st Computer Security Foundations Symposium (CSF); IEEE. 2018

[10] Colnago J, Devlin S, Oates M, Swoopes C, Bauer L, Cranor L, et al., editors. "It's not actually that horrible": Exploring adoption of two-factor authentication at a university. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems; ACM. 2018

[11] Huang X, Xiang Y, Chonka A, Zhou J, Deng RH. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems. 2011;**22**(8):1390-1397

[12] Easttom II WC. Computer Security Fundamentals: Pearson IT Certification; 2019

[13] Nissanke N, Khayat EJ, editors. Risk Based Security Analysis of Permissions in RBAC. WOSIS; 2004

[14] Bonneau J, Herley C, Van Oorschot PC, Stajano F, editors. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy; IEEE. 2012

[15] Forget A, Chiasson S, Biddle R. User-centred authentication feature framework. Information and Computer Security. 2015;**23**(5):497-515

[16] Genero M, Cruz-Lemus J, Piattini M. Métodos de investigación en ingeniería del software. Madrid, Spain: Editorial RA-MA; 2014. pp. 171-199

[17] Kock N, Lau F. Information systems action research: Serving two demanding masters. Information Technology & People. 2001;**14**(1)

[18] Eden C, Ackermann F. Theory into practice, practice to theory: Action research in method development.

European Journal of Operational Research. 2018;**271**(3):1145-1155

[19] Wadsworth Y. What Is Participatory Action Research? Action Research Issues Association; 1993

[20] Padak N, Padak G. Guidelines for planning action research projects. Research to Practice. ERIC. 1994

[21] Kitchenham B. Procedures for performing systematic reviews. Keele, UK, Keele University. 2004;**33**(2004): 1-26

[22] Kitchenham BA, Pfleeger SL. Personal opinion surveys. In: Guide to Advanced Empirical Software Engineering. Springer; 2008. pp. 63-92

[23] Rosqvist T, Koskela M, Harju H. Software quality evaluation based on expert judgement. Software Quality Journal. 2003;**11**(1):39-55

[24] Runeson P, Host M, Rainer A, Regnell B. Case Study Research in Software Engineering: Guidelines and Examples. John Wiley & Sons; 2012

[25] Velásquez I, Caro A, Rodríguez A. Authentication schemes and methods: A systematic literature review. Information and Software Technology. 2018;**94**:30-37

[26] Velásquez I, Caro A, Rodríguez A. Kontun: A framework for recommendation of authentication schemes and methods. Information and Software Technology. 2018;**96**:27-37