Omnifactor Authentication

Libor Dostálek[1], Iva Dostálková[2]

1. Department of Applied Informatics, Faculty of Science, University of South Bohemia, CZECH REPUBLIC, Ceske Budejovice, Branisovska 1760, email: dostalek@prf.jcu.cz

2. Department of Mathematics and Biomathematics, Faculty of Science, University of South Bohemia, CZECH REPUBLIC, Ceske Budejovice, Branisovska 1760, email: dost@prf.jcu.cz

Abstract: **At present, many authors looking for new and new authentication methods [1] [2], which their authors consider that, are stronger and stronger. Individual one-factor authentication methods combine to other, and thus multi-factor authentication will arise. Today's applications typically allow users to choose from a set of supported authentication methods. Users can choose to use one or a combination of multiple authentication methods. We say that users have available omnifactor authentication. The question is how to quantify the strength of the selected methods in kind of omnifactor authentication. This is important to determine if is the authentication sufficient for the required service (required information). This article offers the answer to this question by quantifying authentication based on knowledge, ownership and inherence factors.**

Keywords: **authentication, multifactor authentication, omnifactor authentication.**

I. Introduction

Authentication is the entity's identity verification process. This process is carried out by a verifier who guarantees that the entity has a declared identity (Figure 1). The quality of this warranty depends on the particular authentication process.

We distinguish entity authentication and message authentication. The difference is in the time perspective. Authentication of the message (erg by electronic signature) gives no guarantee as to when the message was created. Instead, entity authentication includes proof of identity of the applicant as a rule through current communication with the verifier.

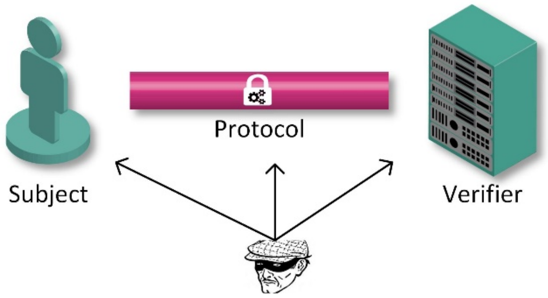

Fig. 1. Fundamental roles in authentication process.

An example of an authentication process is the process by which a user logs on to the application using a username and password.

The secondary effect of the authentication process may be the fact that during the authentication of the entity, cryptographic material will also be generated to serve for subsequent communication.

The ways in which someone may be authenticated fall into three categories, based on what are known as the factors of authentication:

1. The subject something knows - knowledge factors – e.g. password, private or secret key, shared secret, etc.
2. The subject has something - ownership factors – e.g. smart card, one-time passwords token, etc.
3. Subject something is or does - inherence factors – e.g. fingerprint dynamic biometric signature, digital footprint, etc.

Multi factor authentication grant access only after successfully presenting two or more factors (Figure 2).

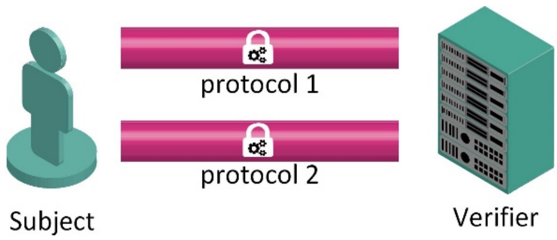

Fig. 2. Multi factor authentication.

It is important that different authentication factors are used. E.g. using two passwords does not improve the authentication quality. Authentication factors may vary:

- Different cryptographic material.
- Different authentication scheme.
- Different communication protocol.
- Different communication channel.
- Different verifier.

It is also important that the authentication factors are intertwined. If they are not, then the attacker makes work easier because the attacker can first deal with breaking one authentication factor and then another. However, this cannot always be achieved. E.g. if an entity is already authenticated (for example, it has brought authentication from Facebook) and it turns out that stronger authentication (e.g. smart card) is required for the operation, then it is usually re-authenticated only with a stronger chip scheme independent of the original authentication. The basic disadvantage of biometric person's characteristics is that they cannot be revoked and subsequently altered in the case of abuse. E.g. if an attacker obtains a dynamic biometric signature from the subject, then the subject can never use a dynamic biometric signature without compromising its misuse.[1]

II. Relate Works

The inherence authentication factors are usually considered as based on the biometric properties of the subject, i.e. verification of the person's identity based on measurable physiological or behavioral characteristics, unique and relatively unchanging for the subject.

Authentication takes place based on the input pattern match pre-stored template e.g. in the database. Matching cannot be absolute - probably, it may be an attack. Authentication is confirmed if the matching exceeds a predetermined threshold.

So far, we have considered authentication as it is used, for example, when logging in to FTP or Telnet server. However, at present, logging is part of wider communication, for example, when a user logs in to a web server. The communication for displaying the logon page transmits a large amount of data and the logged-on user leaves the digital footprint. A digital footprint can be used for authentication itself or can serve as another authentication factor. Interestingly, the information extracted from the digital footprint can not only amplify but also weaken the resulting authentication. Weaken, if are detected potential attack.

If we want to use the digital footprint for authentication, then:

1. From a digital track, we must be able to identify users. The easiest way to do this is to save the user's identification to cookies.
2. Upon subsequent authentication, we can determine the degree of match information in the current digital footprint with information in the previous digital footprints of the same user.
3. If we find a mismatch of the current digital footprint with the previous digital tracks, then we can ask the user for additional (secondary) authentication.

The Digital Footprint has similar features to biometric characteristics. The key is to be able to identify user from the digital track. However, even when digital footprint are able to identify users with a certain probability, it can be useful in practice. It can be used, for example, to distribute a customized ad.

Risk based authentication is called authentication based on the calculation of the likelihood of attack against this authentication. The patent [1] deals with user authentication in the kind of an Internet service provider's application. This can be, for example, an e-shop, electronic banking or eGovernement application. The client during authentication and subsequent downstream communication leaves a lot of information in the communication channel - leaving a digital footprint. The principle is as follows: the communication flow between the subject and the verifier is duplicated. The duplicate of the communication stream is redirected to the Risk Engine, which then evaluates this information as the input information for calculating the risk score (Figure 3). The risk score can then serve as input:

- For risk-based authentication that is used in this paper.
- Fraud detection system, which is used to detect cyber-attacks. The goal is to launch an action based on a voluminous score that either warns of a potential attack (generates risk alerts) or attempts to directly prevent a potential attack (generates risk action).

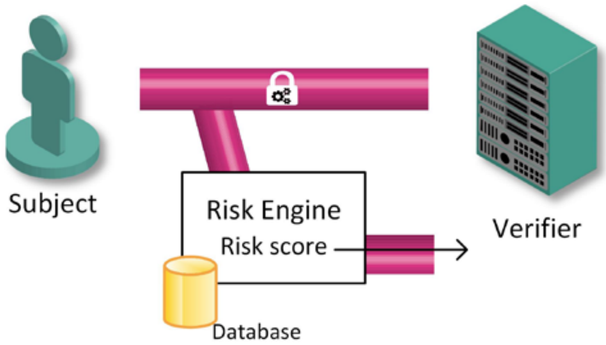

Fig. 3. Risk Based Authentication.

Risk scores can be calculated on the basis of several considerations:

- Risk Engine can accurately monitor the authentication process and detect even minor deviations from this process. These deviations can be caused, for example, by the fact that instead of human authentication the robot (program) trying authentication.
- Comparing the current digital footprint with the history of digital footprint stored in the database. For example, autonomous system (set of IP addresses) from which the user logs in. The version of the software the user uses, etc. This option is being used by the patent [3] and is mentioned in the following text.
- Blacklists.
- Whitelists.

Patent [3] introduces terms:

- “Pre-authentication” as a manner demined both by the identity of the device from which the authentication request originates as well as by available information concerning the identity of the requesting user.
- “Post-authentication” using a user’s transaction history.

Patent [1] gives an interesting example using decision Table 1, table 2 and Table 3. The primary decision table is Table 1 and table 2. Under certain conditions, Table 3 is considered. Score 10 is a likelihood attack, score 0 indicated a low likelihood of attack (fraud).

Patent [1] is tributary for the period in which it was incurred. Currently, users are mainly using mobile applications. For mobile applications, risk-based authentication is even more advantageous. Mobile apps run on a mobile device, so they can read the hardware and software identification of mobile devices and provide risk based authentication. It can therefore provide more information than a web browser.

It is also very important to provide localization data. If the client is authenticated at a short time from two very remote

[1] In the case of the handwriting signature, it is possible to attach a digit, picture, etc. to the signature. This de facto revoke the previous signature without a digit or image.

sites, then it is also poised.

TABLE 1. PRIMARY DEVICE DECISION TABLE

Period	**Criteria**	**Request Attributes**
Pre-authentication	Location information	- City, State, Country information and confidence factors - Connection type Connection speed - IP address, routing type, and hop times - Internet service provider flag - Autonomous system number - Carrier name - Top-level domain - Second-level domain - Registering organization - A list of anonymizing proxies - Hostnames and routers
	Device information	- Secure Cookies - Flash Cookies - Digitally signed device - Device & display Characteristics: - Operating System characteristics - Browser Characteristics
Post-authentication	User information	- User identifications - Valid or not valid user - Authentication status
	Transaction information	- Key Value Pairs: - Support multiples - Keys can be defined using Regular Expressions - Values can be defined in ranges - Pages accessed - Time spent on page - Transactions sequences

III. RISK BASED AUTHENTICATION

The question is how to compare various authentication methods. I propose to use a Risk-based method of comparison. The goal of this method is, if possible, automatically (Online) classify the strength of authentication. The problem is how to quantify the quality of the used authentication. Risk-based authentication uses procedures similar risk analysis. This method starting from empirically prescribed risk level of individual authorization methods. This method does not look too exactly, but during the subsequent evaluation of security incidents ("Feedback") can be risk adjusted, so that over time, this method can be very effective.

TABLE 2. PRIMARY DEVICE DECISION TABLE (SCORE)

Secure cookie	**Flash cookie**	**Flash data**	**Browser characteristics**	**OS characteristics**	**Score**
*	*	*	*	*	0
X	*	*	*	*	PATTERN CHECK
M	*	*	*	*	SECONDARY CHECK
X/M	X	*	*	*	PATTERN CHECK
X/M	M	*	*	*	SECONDARY CHECK
X/M	X/M	X	*	*	PATTERN CHECK
X/M	X/M	M	*	*	SECONDARY CHECK
X/M	X/M	X/M	M	*	SECONDARY CHECK
X/M	X/M	X/M	X/M	M	10

X=Missing, M=present and mismatched, * = present and matched

TABLE 3. SECONDARY DEVICE DECISION TABLE (SECURE COOKIE MISMATCH)

Prior Cookie (same device) Browser Characteristics	**TRUE Operating System**	**autonomous system number**	**Internet service provider**	**IP stands for IP address**	**Location**	**Score**
T	T	T	T	T	T	0
F	T	T	T	T	T	5
X	T	T	T	T	T	5
T	F	T	T	T	T	10
T	X	T	T	T	T	0
T	T	F	T	T	T	10
T	T	X	T	T	T	0
T	T	T	F	T	T	5
T	T	T	X	T	T	0
T	T	T	T	F	T	5
T	T	T	T	X	T	0
T	T	T	T	T	F	5
T	T	T	T	T	X	0
F	F	F	F	F	F	10
X	X	X	X	X	X	10

T=TRUE, F=FALSE, X=Missing

IV. KNOWLEDGE RISK BASED AUTHENTICATION

For the category of authentication as knowledge is practical to use the set of security features. Example of security features in on Table 4.

For each of this security features we express the risk weight v_i of security features number i. To avoid big differences in case of adding new security features, we assume:

$$\sum_{i=1}^{n} v_i = 1$$

For the k-th authentication mechanism shows the security features as the Risk coefficient r_i^k gets 1 or 0 depending on whether or not the security features are met. Quality (strength) of authentication mechanism k can be expressed as:

$$q^k = \sum_{i=1}^{n} v_i \, r_i^k$$

In the example given in Table 4, the result is the value is 0.2.

V. Possession Risk Based Authentication

TABLE 4. Example of security features for knowledge base authentication

	Security features	Classical Password authentication	
		Weight v_i	r_i^k
1	Password change supported	⅒	**0**
2	Password reset supported	⅒	**0**
3	Password eavesdropping is possible	⅒	**0**
4	Password guessing is possible	⅒	**0**
5	Password elicitation is possible	⅒	**0**
6	Time de-synchronization is possible	⅒	**1**
7	Anti-desynchronization	⅒	**0**
8	Data bearer revocation supported	⅒	**1**
9	User anonymity guaranteed	⅒	**0**
10	User un-traceability guaranteed	⅒	**0**

For the category of authentication categorized as possession we can define the set of security features. For example:

- Cryptographic material does not stored in secured environment (data bearer)
- Access to cryptographic material without password or PIN
- Cryptographic material is exportable
- Cryptographic material does not physically protected against unauthorized access

For each of this security features we express the risk weight w_i. And similarly assume that:

$$\sum_{i=1}^{m} w_n = 1$$

For the k-th authentication mechanism we define the Risk coefficient R_i^k, Quality (strength) of authentication mechanism k can be expressed as:

$$Q^k = \sum_{i=1}^{m} w_i R_i^k$$

VI. Inherence Risk Based Authentication

In this category is traditionally considered biometric characteristics of the person. However, the use of biometric characteristics of persons has many disadvantages. Biometric features cannot be revoked, so have many common features with traditional passwords. In addition, biometric authentication brings complications with the protection of personal data.

In this category of authentication, we will mainly consider digital footprint. We will evaluate the correlation between the information from previous communications and the currently identified footprint. The correlation coefficient ρ is from the interval of <-1,1>. Negative values are important when detecting abnormalities in digital track. With them it is possible e.g. when detecting certain abnormal or decrease the overall weight of authorization. We can use method described in [3] but we need to transform the score to match the ρ definition domain <-1,1>.

VII. Omnifactor Authentication

In kind of omnifactor authentication we assume that a user from a set of authentication methods has chosen the method k. The result quality QQ^k is weighted sum of individual categories:

$$QQ^k = W_1^k q^k + W_2^k Q^k + W_3^k \rho^k + ext$$

Wight W_i^k we choose zero in the case that the category is not used and non-zero in case of categories in terms of technology, algorithms and parameters, which ensure increasing quality of authentication. Item ext mean external authentication, they cannot measure, so we have to determine subjectively.

Using weights Wight W_i^k can be taken into account independency of various authentication factor.

VIII. Conclusion

It may seem that the problem is to determine the weights v_i and w_i. However, at the beginning, it can determine the same weight v_i, respectively w_i. Based on the evaluation of security incidents, we can modify individual weight. This will make the model more accurate.

Similarly, we evaluate provided information (services), i.e. assets. If we appreciate an asset, for example, the value of X, then for providing this asset we allow only authentication methods k with

$$QQ^k \geq X$$

It should also be noted that risk-based authentication could also have drawbacks. Can generate False Positives in the usual cases e.g.: the client purchases a new mobile device; the client will forget to make a payment order prior to the holiday and make it out of an exotic country etc.

IX. Further Work

Further work I'll focus on more precise definition of risk weight and simulation of examples. Next problem is re-authentication. It is situation when authenticated does not have sufficient rights and needs to increase score of authentication.

Reference

[1] L. Dostalek a J. Ledvina, „Strong Authentication for Mobile Application,“ *International Conference of Applied Elecronics, č. IEEE CFP1569A-PRT*, pp. 23-26, September 2015.

[2] L. Dostálek, „Srong Authentication for Internet Application,“ v *16th European Conference on Cyber Warfare and Security,* Dublin, 2017.

[3] T. E. Varghese, J. B. Fisher, S. L. Harris a D. D. Boseo, System and Method for Fraud Monitoring, Detection, and Tired User Authentication, Patent N0.: US 7,908,645 B2, 2011.