ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

PROGRESSIVE INFORMATION TECHNOLOGIES

ПРОГРЕССИВНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

UDC 004.738

MULTI-FACTOR AUTHENTICATION MODELLING

Dostálek L. – M.Sc., Post-graduate student at the Department of Computer Science and Engineering, University of West Bohemia Pilsen, Czech Republic.

Šafařík J. – PhD, Professor, Professor of the Department of Computer Science and Engineering, University of West Bohemia Pilsen, Czech Republic.

ABSTRACT

Context. Currently, institutions and companies face massive cyber-attacks. Attacks are always focused on some authentication weakness that is part of a particular authentication protocol. In the event of an attack, it is necessary to respond flexibly to the weakening of authentication mechanisms. In the event of an attack, it is necessary to quickly identify the affected authentication factor and its importance to temporarily weaken. Subsequently, it is possible to detect the affected weakness and weaken the meaning of only the algorithms showing this weakness. Algorithms that do not show this weakness should be left unchanged. This paper introduces a mathematics model of authentication. By quick changing the model parameters, we can flexibly adapt the use of authentication means to the situation.

Objective. The purpose of this work is to propose a method that will allow to quantify the strength (quality) of authentication. In order it will be possible to dynamically change the authentication method depending on the current risks of attacks.

Method. The method is to design a mathematical model and its simulation. The model is then based on the sum of the strengths of the individual authentication factors. A risk-based mechanism is used to determine model parameters.

Results. The paper then demonstrates the simulation results using commonly used authentication means. The paper then demonstrates the simulation results using commonly used authentication means: password, hardware based one-time password, device fingerprint, external authentication, and combination of this methods. Simulations have shown that using this mathematical model makes it easy to model the use of authentication resources.

Conclusions. With this model, it seems easy to model different security situations. In the real situation, the model parameters will need to be refined as part of the feedback assessment of the established security incidents.

KEYWORDS: authentication, multifactor authentication, risk-based authentication, omnifactor authentication, fraud detection system, password, digital fingerprint

ABBREVIATIONS

FDS is Fraud Detection System;

CSIRT is Security Incident Response Team;

NOMENCLATURE

n is number of the classification level information;

K is a concrete authentication method;

$risk_{max}$ is the maximal value of assessed risks;

F_{know}^{K} is an authentication factor based on knowledge;

F_{own}^{K} is an authentication factor based on ownership;

F_{inh}^{K} is an authentication factor based on inherence;

F_{ext}^{K} is an external authentication factor;

q_{know}^{K} is the quality (strength) of the authentication factor based on knowledge;

q_{own}^{K} is the quality (strength) of the authentication factor based on ownership;

q_{inh}^{K} is the quality (strength) of the authentication factor based on inherence;

q_{ext}^{K} is the quality (strength) of an external authentication factor;

q^{K} is a quality of the authentication method K;

W_{know}^{K} is the weight of the authentication factor based on knowledge;

W_{own}^{K} is the weight of the authentication factor based on ownership;

W_{inh}^{K} is the weight of the authentication factor based on inherence;

DOI 10.15588/1607-3274-2020-2-11

W_{ext}^{K} is the weight of an external authentication factor;

n_{know}^{K} are the risks of authentication factors are the characteristics (features) of specific authentication factors.

INTRODUCTION

Authentication is the process of verifying the identity of the subject. This process makes it possible to identify a person or to confirm the origin of the data message. This process is performed by a verifier who guarantees that the entity or origin has a declared dentity (Fig. 1).The quality of this guarantee depends on the specific authentication process. And also depends on participants of the authentication process. The aim of this work is to model the quality of authentication process.

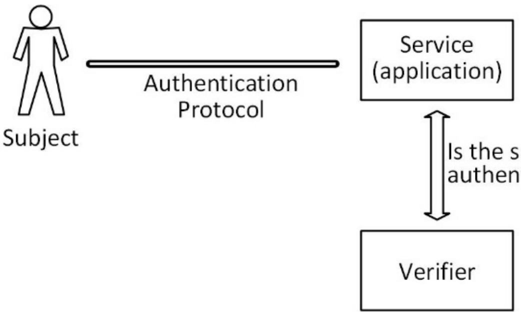

Figure 1 – Participants in authentication process

The person is usually authenticated at the beginning of the session. The difference between session and data message authentication is in the time perspective. When a subject authenticates itself at the beginning of the session, e.g. with help of name and password, then usually the authentication is valid for the duration of the whole session. We can then investigate if over time this method of authentication retains its quality or not. By contrast, the data message is authenticated or not.

The side effect of the authentication may be generation of cryptographic material for securing subsequent communication. This is the features of only some authentication algorithms. Unfortunately, in most cases, today's cryptographic security material for session securing is generated randomly before its own authentication (so-called ephemeral cryptographic material). Authentication will take place within this beforehand secured channel.

The principle of authentication fall into one of three well known authentication factors:

The knowledge factor ("the subject something knows"). If the knowledge is based on information knowledge, the quality of this authentication factor often depends on the entropy of that information. Of course, the quality of this authentication depends as well on the cryptographic algorithm used and participants of authentication.

The ownership factor ("the subject has something"). In this case, the quality of authentication, inter alia, depends on how "something" has subject under its sole control.

The inheritance factor ("the subject something is or does"). While the previous two authentication factors are obvious. The inheritance authentication factor has been very interesting lately. Historically, this authentication factor to mean human biometrics. In recent years, however, is more investigated the behavior of the subject and the fingerprint of device used by the subject.

More recently, authentication by external providers is being as well used (e.g. Google). External authentication often uses OAuth 2.0 and OpenID Connect protocols. In the case of this external authentication, we will not investigate what factors it is based on. We will look at external authentication as a black box, and for the purposes of the model described below we will consider it as a separate forth authentication factor.

In the case of multifactor authentication, it is also important that used authentication factors are mutually interlinked. If authentication factors are completely independent, an attacker can attempt to break each of the factors used independently of each other. This will simplify the effort of an attackers.

Unfortunately, it is not possible to require interlinking of authentication factors if, as an authentication factor, we use external authentication. This is also not possible in case of re-authentication. I.e. in the event that an authenticated subject during its session will require access to resources that require stronger authentication than authenticated at the beginning of the session.

If the application provider allows the user to authenticate themselves with several different authentication tools. Then we talk about omnifactor authentication [1]. The goal of our model is to choice optimal authentication tools for accessing specifically classified resources provided by the application.

The subject uses authentication to gain access to assets (e.g. information assets) that will be classified to levels 1 to n for the needs of our model (Fig. 2). Assets can be classified, for example, by the asset's carrying amount. However, it is more likely to be based on the risk analysis mentioned below.

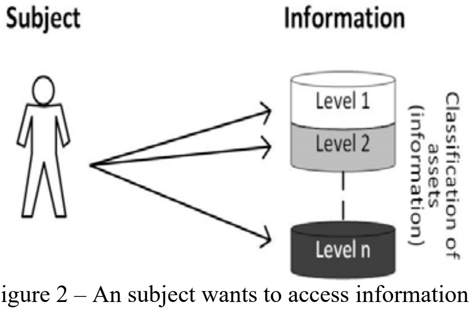

Figure 2 – An subject wants to access information (assets) classified to level information i, where $i=1,\ldots n$

The question is, what authentication method is sufficient to access the classification level information i, where $i=1,\ldots n$. The solution described below is to use the Risk Based Authentication principle. This paper

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

introduces an authentication model that determines whether the authentication is sufficient for a specified level of classification based on the input parameters.

The object of study is the process of authentication to access information with concrete classification.

The subject of study is multi-factor authentication methods and models.

The purpose of the work is to defines a multi-factor authentication model in case the application supports multiple authentication measures, which allows for a flexible response to the changed security situation.

1 PROBLEM STATEMENT

The problem is that at present miss models that dynamically model the required strength of authentication on the basis of individuality methods, or on the basis of current security situation.

To design such a model, I first need to quantify the strength of authentication methods. To this end, we define the quality of the authentication method using a risk-based mechanism.

Let us have the assets valued at levels 1 through n. Now we have a concrete authentication method K. The task is whether the authentication method K is sufficient to access the assets of the classification level information i, where $i = 1, \ldots n$.

The authentication method K is generally multifactor authentication method, which may consist of authentication factors: F_{know}^{K}, F_{onw}^{K}, F_{inh}^{K} a F_{ext}^{K}. Where:

Authentication factor F_{know}^{K} is based on knowledge. Quality (strength) of this authentication factor we evaluate by value q_{know}^{K}.

Authentication factor F_{onw}^{K} is based on ownership. Quality (strength) of this authentication factor we evaluate by value q_{onw}^{K}.

Authentication factor F_{inh}^{K} is based on inherence. Quality (strength) of this authentication factor we evaluate by value q_{inh}^{K}.

Other authentication factor F_{ext}^{K}, e.g. external authentication. Quality (strength) of this authentication factor we evaluate by value q_{ext}^{K}.

Overall, we evaluate the authentication method K by value q^{K}:

$$q^{K} = W_{know}^{K} q_{know}^{K} + W_{own}^{K} q_{own}^{K} + W_{inh}^{K} q_{inh}^{K} + W_{ext}^{K} q_{ext}^{K}.$$

Weights W_{know}^{K}, W_{own}^{K}, W_{inh}^{K} and W_{ext}^{K} we choose zero in the case that the authentication factor is not supported and non-zero in case of categories in terms of technology, algorithms and parameters, which ensure increasing quality of authentication. Using this weights can be taken into account dependency or independency of various authentication factor. Weights W_{know}^{K}, W_{own}^{K}, W_{inh}^{K} and W_{ext}^{K} we will use in case of attack simulation. We will mention this weights W_{know}^{K}, W_{own}^{K}, W_{inh}^{K} and W_{ext}^{K} in the chapter Simulation.

We will now look at how to determine the values: q_{know}^{K}, q_{own}^{K}, q_{inh}^{K} and q_{ext}^{K}.

2 REVIEW OF THE LITERATURE

None of the authentication methods is perfect. The effort is to seek new and new authentication methods or to augment existing ones. But we will follow a different path. We will classify existing methods and see if they are appropriate for the situation.

Device Fingerprinting means collecting information about a computing system and its communication that may lead to device identification or at least partial identification. In practice, however, the device fingerprint typically detects a user communicating from a specific device. I.e. gathering information not only about the hardware and software installed on the device, but also about its user configuration and, if applicable, the behavior of a particular user.

The server can collect a wide range of client communication information based on various methods that can characterize a particular device, and therefore assume that the device is being used by a specific user. Individual methods are referred to as device fingerprinting vectors. Such fingerprinting vectors can be, for example, information about the device software, operating system version type including its version, or information provided by the browser (e.g., cookie) or the time zone set, etc. E.g. [2] defines 29 fingerprinting vectors that classify into four categories: Browser provided information, Inference based on device behavior, Extensions and plugins and Network and protocol techniques. It also states five basic types of attacks on device fingerprinting. The paper [3] uses fingerprinting vectors based on motion Sensors. There are a number of such articles [4–5]. Their deficiency is that they identify individual authentication factors, but they do not specify to qualify their authentication strength somehow in order to be somehow comparable.

The FDS principle is the opposite of authentication. FDS calculates the likelihood of a successful attack against authentication. It's not a whole new approach. Patent [4] has already applied this idea to Internet applications.

FDS typically introduces a client behavior model and classifies deviations from this model. The article [5] classify different approaches in FDS (Data Mining, Artificial Intelligence, Machine Learning, Genetic Programming, Reinforcement Learning, Transformed-domain-based and Combined Criteria).

By the term Risk-based authentication, we mean authentication taking into account the risk of a successful attack against this authentication. Historically, patent [4]

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

assumed that FDS methods and authentication methods may sometimes use the same principles. More recent work has already been mentioned [2] which defines 29 fingerprinting vectors that classify into four categories.

A risk-based authentication scheme is illustrated in the (Fig. 3). The communication between the subject and the application is intercepted. The duplicated communication stream is evaluated by Risk Engine. The Risk Engine will uses knowledge database to evaluate the behavior of the subject and calculate device fingerprint. Sometimes it does not evaluate the behavior of individual subjects, but group of subjects that contains equivalent subjects in terms of this evaluation (e.g. domestic customers, foreign customers, corporate customers etc.). The result of the evaluation is value Risk score. On the value of the Risk Score depends the decision of Verifier whether the subject is authentic or not, i.e. whether the authentication is successful or not.

The Patent [4] of the Authentication Assessment essentially carries out a decision based on something that reminds the decision tree. The article [2], in turn, makes the assessment on the basis of a penalty. We will make the decision on the basis of a standardized risk analysis built on the standard [6].

Risk analysis is today a very common technique. This can be done, for example, based on the standard [6]. This standard:

Performs identification of assets. Which can lay down for us classification of information.

Evaluates the risks. The resulting risk value is the product of the threats assessment, vulnerabilities assessment, and impacts of assessed risks.

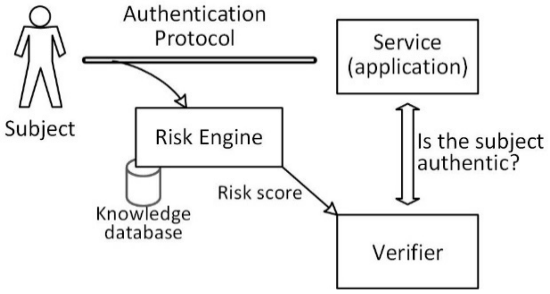

Figure 3 – Risk Based Authentication

For evaluation of threats assessment, vulnerabilities assessment, and impacts of assessed risks we will use scale from 1 to $risk_{\max}$. For the purposes of this work, we will use the scale 1 to 4 (Low, Medium, High or Critical) as an example. The resulting risk is then the product threats, vulnerabilities and impact of risks. I the case of scale 1 to 4 the maximal risk value can be up to 64 (=4.4.4). The range of 64 values is very fine for the high level decision. So, for the high level decision, the interval from 1 to 64 we will again divide into 4 parts that again uses scale 1 to 4 corresponded to the risks Low, Medium, High or Critical.

3 MATERIALS AND METHODS

We now think about Knowledge Based Authentication in general. This authentication is based on the knowledge under which we can imagine a password, for example. However, we will now abstain from a specific authentication method. We determine risks of this authentication factor based on a risk analysis performed for a specific application (specific institution).

Risks of authentication factor are the characteristics (features) of specific authentication factors. E.g. for an application (institution) we assume n_{know} risks $know_i$ in Table 1.

Next risks (not included in the table) can by for example in case of generating cryptographic material for securing subsequent communication:

Key freshness – neither party can predetermine the shared session key being established.

Perfect forward secrecy – attacker cannot know any information about previously established session key even when the long-term keys of the server and the user are disclosed.

We now perform risk assessment of individual risks, for example, on scales 1 through 4 (column Risk score r_{knowi} of Table 1) to determine the risk score r_{knowi} for specific risk $know_i$. The risk assessment is that we ask what the risk is for a specific application (institution). The higher the risk, the higher the risk score. The value of risk score is based on a subjective assessment specific situation as is common when performing risk analysis [6].

Based on the risk score, we determine n_{know} risk weights $w^K_{know_i}$ of the individual risks. The weight $w^K_{know_i}$ of specific risk $know_i$ we will define as:

$$w_{know_i} = \frac{r_{know_i - 1}}{(risk_{\max} - 1) \cdot n_{know}}.$$

In our example:

$$w_{know_i} = \frac{r_{know_i - 1}}{3 \cdot n_{know}}.$$

This will ensure that the sum of all weight for a particular authentication factor can be at most 1. This is because if we add additional risks to the model so that the model does not give diametrically different results. The maximum risk one corresponds to the situation as if the authentication factor was not supported at all.

We will now deal with a specific authentication factor F^K_{know}. I.e. we will want the authentication factor F^K_{know} to be valued by q^K_{know} express the strength of the authentication factor. We determine the value q^K_{know} based on the risks of risk-based factor of a concrete authentication method. Generally, for most authentication method, all our identified risks are not up to date.

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

Therefore, we define the variable $p^K_{know_i}$, which for each risk $know_i$:

– will get value 1 if the risk r_{know_i} for the authentication factor F^K_{know} is up to date;

– will get value 0 if the risk r_{know_i} for the authentication factor F^K_{know} is not up to date.

Value q^K_{know} of authentication factor F^K_{know} will be define as:

$$q^K_{know} = 1 - \sum_{i=1}^{n^K_{know}} w_{know_i} \, p^K_{know_i} \ .$$

The maximum value of is one. From value one we subtract the weight of specific risks. I.e. specific risks reduce assessment of the strength of the authentication factor.

The Table 2 shows two simple examples of setting value q^K_{know} for password and one-time password generated by hardware token (only for knowledge base factor – does not include a possession-based factor).

Possession Risk Based Authentication we deal like the Risk Knowledge Based Authentication. I.e. we will use a risk analysis to assess the risks of the authentication factor F^K_{own}. Possession base authentication factor is often based of possession of environment of cryptographic material including data bearer of cryptographic material (e.g. smartcard, Hardware Security Module etc.).

For the category of possession authentication we define on Table 3 similarly the n_{poss} of security risk r_{poss_i}.

Table 1 – An example of risk analysis of knowledge based authentication $(1 \le i \le n_{know})$

i	**Security risks** $know_i$	**Risk score** r_{know_i} **(1–4)**	**Weight** w_{know_i}
1	The knowledge have an information entropy lower than the specified limit.	4	0.08
2	The validity of knowledge is not time limited	3	0.06
3	Knowledge can be used multiple times (not one-time)	4	0.08
4	The number of attempts to guess knowledge is not limited	4	0.08
5	Change of knowledge is not supported	4	0.08
6	Reset of knowledge is not supported	4	0.08
7	The knowledge eavesdropping is possible	4	0.08
8	The knowledge guessing is possible	4	0.08
9	The knowledge elicitation is possible	3	0.06
10	Authentication requires time synchronization	1	0.00
11	Authenticated subject anonymity is not guaranteed	2	0.03
12	Authenticated subject traceability is possible	2	0.03

Table 1 – Examples of values q^K_{know} for a standard password and a one-time password

i	Security risks	Risk score r_{know_i} (1–4)	Weight w_{know_i}	Password		HW based one-time password	
				$p^{Pass}_{know_i}$	$w_{know_i} \, p^{Pass}_{know_i}$	$p^{HW}_{know_i}$	$w_{know_i} \, p^{HW}_{know_i}$
1	The password have an information entropy lower than the specified limit.	4	0.08	0	0.00	1	0.08
2	The validity of password is not time limited	3	0.06	0	0.00	0	0.00
3	Password can be used multiple times (not one-time)	4	0.08	1	0.08	0	0.00
4	The number of attempts to guess password is not limited	4	0.08	0	0.00	0	0.00
5	Change of password is not supported	4	0.08	0	0.00	1	0.08
6	Reset of password is not supported	4	0.08	0	0.00	1	0.08
7	The password eavesdropping is possible	4	0.08	1	0.08	1	0.08
8	The password guessing is possible	4	0.08	1	0.08	1	0.08
9	The password elicitation is possible	3	0.06	1	0.06	1	0.06
10	Authentication requires time synchronization	1	0.00	0	0.00	0	0.00
11	Authenticated subject anonymity is not guaranteed	2	0.03	1	0.03	1	0.03
12	Authenticated subject traceability is possible	2	0.03	1	0.03	1	0.03
Summa					0,36		0,53
				$q^{Pass}_{know_i}$	0,64	$q^{HW}_{know_i}$	0,47

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

Again we perform risk assessment of individual risks, for example, on scales 1 through 4 (otherwise may be different) to determine the risk score r_{poss_i} for specific risk $poss_i$ is that we ask what the risk is for a specific application (institution). The higher the risk, the higher the risk score. The value of risk score is based on a subjective assessment specific situation as is common when performing risk analysis [6].

Similarly to knowledge based authentication, we will establish risk weights $w^K_{poss_i}$:

$$w_{poss_i} = \frac{r_{poss_i}-1}{(risk_{\max}-1)\cdot n_{poss}}.$$

In our example:

$$w_{poss_i} = \frac{r_{poss_i}-1}{3\cdot n_{poss}}.$$

Next we establish variable $p^K_{poss_i}$ and value q^K_{poss} of authentication factor F^K_{poss} will be define as:

$$q^K_{poss} = 1 - \sum_{i=1}^{n_{poss}} w_{poss_i} p^K_{poss_i} .$$

In this category is traditionally considered biometric characteristics of the person. In case of biometric authentication the coefficient q^K_{inh} can be determined, for example, as the percentage of match of actually captured biometric pattern with the saved pattern in database. Such agreement may be for example 0.93 (i.e., 93%).

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.

We will next to deal with the inheritance authentication based on device fingerprinting. Inheritance Risk Based Authentication we deal like the Risk Knowledge Based Authentication. I.e. we will use a risk analysis to assess the risks of the authentication factor F^K_{inh}. For the category of inheritance authentication we define similarly the set of security risk. For example most device fingerprint vectors from [2] are listed in Table 4.

Again we perform risk assessment of individual risks, for example, on scales 1 through 4 (otherwise may be different) to determine the risk score r^K_{inhi} for specific risk inh_i is that we ask what the risk is for a specific application. The value of risk score is based on a subjective assessment specific situation as is common when performing risk analysis.

Similarly to knowledge based authentication, we will establish risk weights w_{inh_i} :

$$w_{inh_i} = \frac{r_{inh_i}-1}{(risk_{\max}-1)\cdot n_{inh}}.$$

In our example:

$$w_{inh_i} = \frac{r_{inh_i}-1}{3\cdot n_{inh}}.$$

Next we establish variable $p^K_{poss_i}$ and value q^K_{poss} of authentication factor F^K_{poss} will be define as:

$$q^K_{inh} = 1 - \sum_{i=1}^{n_{inh}} w_{inh_i} p^K_{inh_i} .$$

External authentication is provided by various providers. A concrete subject will use external authentication from one provider at most. We perform risk assessment of individual external authentication providers, for example, on scales 1 through 4 (practically 1 to 3 because 4 is critical and it is not acceptable) to determine the risk score $r^K_{ext_i}$ of specific provider ext_i.

Since the subject uses at most one authentication provider at a time, then we define the risk weight $w^K_{ext_i}$:

$$w^K_{ext_i} = \frac{r_{ext_i}-1}{risk_{\max}-1}.$$

In our case:

$$w^K_{ext_i} = \frac{r_{ext_i}-1}{3}.$$

In this case, we do not need to use the variables p. Value q^K_{ext} of authentication factor q^K_{ext} will be define as:

$$q^K_{ext} = 1 - w_{ext_i} .$$

4 EXPERIMENTS

We performed the experiment using a simulation. The application provider (the institution) supplies the subjects the following authentication means:

– Password;
– Hardware based one-time password;
– Device fingerprint;
– External authentication from Facebook;
– Combination of: Password + Device fingerprint;
– Combination of: Password + Device fingerprint+ External authentication from Facebook.

The question is by what means the subject gets to which information (Fig. 4).

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

$$q^K = W^K_{know}q^K_{know} + W^K_{own}q^K_{own} + W^K_{inh}q^K_{inh} + W^K_{ext}q^K_{ext}.$$

Wight W^K_i we choose zero in the case that the category (authentication factor) is not up to date for category K and non-zero in case of categories in terms of technology, algorithms and parameters, which ensure increasing quality of authentication.

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

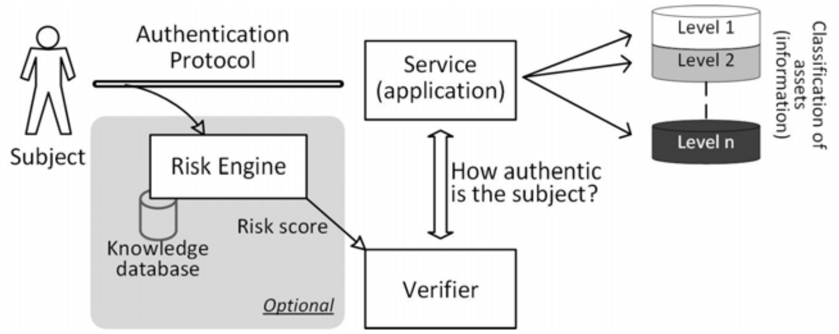

Figure 4 – The subject requests access to the information of a particular classifiction

Application (institution) using n authentication method K_i, where $1 \le i \le n$.

Individual authentication factors can be combined, but q^K can not exceed the sum of the highest possible values of each authentication factor:

$$\max_{1\le i\le n} q^K \le \max_{1\le i\le n} q_{know}^{K_i} + \max_{1\le i\le n} q_{own}^{K_i} + \max_{1\le i\le n} q_{inh}^{K_i} + \\ + \max_{1\le i\le n} q_{ext}^{K_i} .$$

Assets (information) are classified on a scale of 1 to n (see Fig. 2). The task is whether the concrete authentication method is sufficient to access the assets of the classification level information j, where $1 \le j \le n$. So, interval 0 to $\max\limits_{1\le i\le n} q^{K_i}$ must be divided into n parts (the number of classified levels). Intervals may not be the same length, but for the sake of simplicity we will consider equally long intervals (it depends on the assessment of assets [6]). For those intervals for which q^{K_i} will be greater than or equal of these intervals, the authentication method K_i will be sufficient, otherwise not. (In our example is $\max\limits_{1\le i\le n} q^{K_i} = 2.99$).

5 RESULTS

In simulation I we will use the classification of individual resources from the above examples. We do not consider any attack, therefore weight W_{know}^K, W_{own}^K, W_{inh}^K and W_{ext}^K we choose zero in the case that the authentication factor is not supported and one if is supported. In Table 6 we see the result. “Yes” means that for a given level of classification is specific authentication means sufficient. “No” means that there is insufficient.

In Simulation II attacks are being conducted today in campaigns. The application provider (institution), through the exchange of information through the Computer Security Incident Response Team (CSIRT) [7], learns that the current campaign is attacking knowledge base authentication. Therefore in first step, for all means, K sets:

$$W_{know}^K = 0 ,\ \forall_K .$$

We see the result in the Table 7.

In the next step (simulation III), the application provider will find out exactly what kind of attack it is going to take. It was found that the attack was a tapping of long-term passwords. A risk analysis was carried out, while using long-term passwords is risky, but the institution is willing to accept a 30% risk. I.e. W_{know}^K will be changed to 0.30 for long-term password algorithm. (It should be noted that there are also so-called strong password-based authentication methods (mentioned in [8–9]) that will be immune to the actual attack, and the values may come back as they were before the attack.)

After decreasing W_{know}^K to 0.30 we get the values listed in Table 8.

Table 2 – An example of risk analysis of possession based authentication $(1 \le i \le n_{poss})$

i	Security risks $poss_i$	Risk score r_{poss_i} (1–4)	Weight w_{poss_i}	Example: HW based one-time password	
				$p_{know_i}^{HW}$	$w_{know_i} p_{know_i}^{HW}$
1	Cryptographic material does not stored on data bearer in secured environment	4	0.17	0	0.00
2	Access to cryptographic material without any authentication	4	0.17	0	0.00
3	Whole secure environment is not physically protected	4	0.17	1	0.17
4	Cryptographic material is exportable	3	0.11	1	0.11
5	Cryptographic material does not physically protected against unauthorized access	3	0.11	0	0.00
6	Data bearer revocation not supported	2	0.06	1	0.06
Suma					0.33
				$q_{know_i}^{Pass} =$	0.67

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

Table 3 – An example of risk analysis of inheritance based authentication $(1 \le i \le n_{inh})$

i	Security risks inh_i Device fingerprint vector doesn't match:	Risk score r_{inh_i} (1–4)	Weight w_{inh_i}	Example device fingerprint	
				$p^{HW}_{inh_i}$	$w_{inh_i} p^{HW}_{inh_i}$
1	Major software and hardware details	3	0.04	1	0.07
2	System time and clock drift	4	0.07	1	0.07
3	Battery information	4	0.07	1	0.07
4	Evercookies	4	0.07	1	0.07
5	Password autofill	4	0.07	1	0.02
6	Hardware sensors	2	0.02	1	0.02
7	CSS feature detection	2	0.02	0	0.00
8	JavaScript standards conformance	2	0.02	0	0.00
9	URL scheme handlers	2	0.02	0	0.00
10	Video RAM detection	3	0.04	0	0.00
11	Browser plugin fingerprinting	2	0.02	0	0.00
12	IP address	2	0.02	0	0.00
13	Geolocation	2	0.02	0	0.00
14	Counting hosts behind NAT	2	0.02	1	0.00
15	Transaction information is suspicious	1	0.00	1	0.07
Suma					0.31
				q^{HW}_{inh} =	0.69

Table 4 – External Risk-based authentication (example)

i	Security risks ext_i Authentication of the below listed providers will be risk assessed:	Risk score $r^{K}_{ext_i}$ (1–4)	Weight $w^{K}_{ext_i}$	q^{K}_{ext}
1	Google	2	0.33	0.67
2	Facebook	1	0.00	1.00
3	Provider 3	2	0.33	0.67
4	Provider 4	3	0.67	0.33

Table 5 – Simulation: data used from the above examples

				Password	HW based one-time password	Device fingerprint	Facebook	Password + Device fingerprint	Password + Device fingerprint + Facebook
q_{know} =				0.64	0.47			0.64	0.64
q_{poss} =					0.67				
q_{inh} =						0.69		0.69	0.69
q_{ext} =							1.00		1.00
q =				0.64	1.14	0.69	1.00	1.33	2.33
Classification level	8	>	2.62	No	No	No	No	No	No
	7	>	2.25	No	No	No	No	No	Yes
	6	>	1.87	No	No	No	No	No	Yes
	5	>	1.50	No	No	No	No	No	Yes
	4	>	1.12	No	Yes	No	No	Yes	Yes
	3	>	0.75	No	Yes	No	Yes	Yes	Yes
	2	>	0.37	Yes	Yes	Yes	Yes	Yes	Yes
	1	>	0.00	Yes	Yes	Yes	Yes	Yes	Yes

Table 6 – First step in campaign attacking knowledge base authentication.

				Password	HW based one-time password	Device fingerprint	Facebook	Password + Device fingerprint	Password + Device fingerprint + Facebook
q_{know} =									
q_{poss} =					0.67				
q_{inh} =						0.69		0.69	0.69
q_{ext} =							1.00		1.00
q =				0.00	0.67	0.69	1.00	0.69	1.69
Classification level	8	>	2.62	No	No	No	No	No	No
	7	>	2.25	No	No	No	No	No	No
	6	>	1.87	No	No	No	No	No	No
	5	>	1.50	No	No	No	No	No	Yes
	4	>	1.12	No	No	No	No	No	Yes
	3	>	0.75	No	No	No	Yes	No	Yes
	2	>	0.37	No	Yes	Yes	Yes	Yes	Yes
	1	>	0.00	No	Yes	Yes	Yes	Yes	Yes

DOI 10.15588/1607-3274-2020-2-11

Table 7 – $W_{know}^{Password}$ decreased to 0.30

				Password	HW based one-time password	Device fingerprint	Facebook	Password + Device fingerprint	Password + Device fingerprint + Facebook
$q_{know} =$				0.30	0.30			0.30	0.30
$q_{poss} =$					0.67				
$q_{inh} =$						0.69		0.69	0.69
$q_{ext} =$							1.00		1.00
$q =$				0.19	1.14	0.69	1.00	0.88	1.88
Classification level	8	>	2.62	No	No	No	No	No	No
	7	>	2.25	No	No	No	No	No	No
	6	>	1.87	No	No	No	No	No	Yes
	5	>	1.50	No	No	No	No	No	Yes
	4	>	1.12	No	Yes	No	No	No	Yes
	3	>	0.75	No	Yes	No	Yes	Yes	Yes
	2	>	0.37	No	Yes	Yes	Yes	Yes	Yes
	1	>	0.00	Yes	Yes	Yes	Yes	Yes	Yes

6 DISCUSSION

If it is not possible to dynamically model the use of authentication methods, then in the event of an attack, applications must be stopped and re-configured. This leads to application failures.

In [9] we published the first model that assumed that risk analysis would be performed for each method of authentication. In this article, we have already concluded that it is enough to do a risk analysis of within the application (institution) only for each authentication factor. The risk analysis result is then common to each authentication method. This greatly simplifies modeling.

The work [10] deals with cloud services authentication. We believe that the method we propose will be suitable for this type of service.

CONCLUSIONS

The model allows users to work effectively with user authentication when the application provider provides multiple authentication means of different strengths. In addition the model allows quickly respond to emerging security situations.

The values q are set based on the risk analysis of the authentication algorithms. On the other hand, weights W, which are also set in the interval of 0 to 1, correspond to the risk of the current security situation. Both the q and the W values may be practically be corrected based on feedback after an assessment of potential security incidents.

The scientific novelty lies in the idea of modeling the use of authentication methods. In [9] presented the model, we simplified the risk analysis only for the whole application (institution) and not for each authentication factor.

The practical significance is that the use of authentication means can be dynamically modeled.

If we do not use the model, but the individual authentication mechanisms are implemented “hard”, then in the case of an attack the corresponding countermeasures will take a long time and will be clumsy. This model allows dynamically respond to various emergencies.

Simulated was the attack on knowledge based authentication. Similarly, the model can be used for other types of attack.

At present, the most common incident detected by the FDS is that the user buy new computer / mobile. Or that he travels to a vacation in a distant country and suddenly his approach seems suspicious. At this point, the user is usually intricately contacted to verify if an attack occurs. This requires considerable costs. Using this model, application can automatically request stronger authentication from the user. This reduces user service costs.

Prospects for further research. The values q^K is evaluated by at the moment of authentication, ie at time 0 after authentication. However, we must be aware that with increasing time, the risk of a successful attack on an authenticated session increases. It would not be seen the W_i^K as a value, but as a function $W_i^K(t)$ of time t from the start of authentication. The question is, how this function should decrease.

ACKNOWLEDGEMENTS

This work was partially supported by University specific research project SGS-2019-016 Synthesis and Analysis of Geometric and Computing Models.

REFERENCES

1. Dostálek L., Dostálková I. Omnifactor Authentication, *Advanced Computer Information Technologies: International Conference ACIT 2018, Ceske Budejovice, 1–3 June 2018: proceedings*. Ternopil, TNEU, 2018, pp. 228–231.
2. Alaca F., Oorschot P. C. Device fingerprinting for augmenting web authentication: classification and analysis of methods, *Computer Security Applications: the 32nd Annual Conference ACSAC '16, Los Angeles, California,*

© Dostálek L., Šafařík J., 2020
DOI 10.15588/1607-3274-2020-2-11

USA, 2016: proceedings. Los Angeles, California, USA, 2016, pp. 289–301. DOI: https://doi.org/10.1145/2991079.2991091

3. Yang Z., Zhao R., Yue C. Effective Mobile Web User Fingerprinting via Motion Sensors, *Trust, Security And Privacy In Computing And Communications: 17th IEEE International Conference / Big Data Science And Engineering: 12th IEEE International Conference, 1–3 Aug. 2018: proceedings*. New York, NY, USA, 2018, pp. 1398–1405. DOI: 10.1109/TrustCom/BigDataSE.2018.00194
4. Arya V., Sethi D., Paul J. Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing, *International Journal of Information Management,* 2019, Vol. 49, pp. 142–156. https://doi.org/10.1016/j.ijinfomgt.2019.03.013
5. Hinds J., Joinson A. Human and Computer Personality Prediction from Digital Footprints, *Current Directions in Psychological Science,* 2019, Vol. 28, Issue 2, pp. 204–211. https://doi.org/10.1177%2F0963721419827849
6. Varghese T. E., Fisher J. B., Harris S. L., Boseo D. D. Pat. US7,908,645B2 US, H04L63/20, System and Method for Fraud Monitoring, Detection, and Tired User Authentication/ (US), applicant Oracle International Corporation. № 11/412,997; 28.04.2006; 14.12.2006, 51p.
7. Carta S., Fenu G., Recupero D., Saia R. Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model, *Journal of Information Security and Applications*, 2019, Vol. 46, pp. 13–22.
8. Information technology Security techniques – Information security risk management: ISO/IEC 27005:2018. [Effective from 2018-07], 2018, 56 p.
9. Dostálek L., Multi-Factor Authentication Modeling, *Advanced Computer Information Technologies: 9th International Conference ACIT'2019, Ceske Budejovice, Czech Republic, 5–7 June 2019: proceedings.* Ternopil, TNEU, 2019, pp. 443–446. DOI: 10.1109/ACITT.2019.8780068.
10. Vijaya C. J., Challa N., Pasupuletti S. K. Authentication and authorization mechanism for cloud security, *International Journal of Engineering and Advanced Technology*, August 2019, Volume 8, Issue 6, pp. 2072–2078, E-ISSN:2249-8958

Received 01.09.2019.
Accepted 20.04.2020.

УДК 004.738

МОДЕЛЮВАННЯ МУЛЬТИФАКТОРНИХ АВТЕНТИКАЦІЙ

Досталек Л. – магістр, аспірант кафедри комп'ютерних наук та інженерії, Університет Західної Богемії в Плзні, Чехія.

Шафарік Й. – канд. техн. наук, професор, професор кафедри комп'ютерних наук та інженерії, Університет Західної Богемії в Плзні, Чехія.

АНОТАЦІЯ

Актуальність. У даний час, установи та компанії стикаються з масовими кібератаками. Атаки завжди зосереджені на деякій слабкості аутентифікації, яка є частиною конкретного протоколу аутентифікації. У разі нападу необхідно гнучко реагувати на ослаблення механізмів аутентифікації. У разі нападу необхідно швидко визначити постраждалий фактор аутентифікації та тимчасово послабити його значення. Згодом можна виявити уражену слабкість і послабити значення лише алгоритмів, що проявляють цю слабкість. Алгоритми, які не проявляють такої слабкості, слід залишити без змін. У цій роботі представлена математична модель аутентифікації. Швидко змінюючи параметри моделі, ми можемо гнучко адаптувати використання засобів аутентифікації до ситуації.

Мета – запропонувати метод дозволяє кількісно оцінити силу (якість) аутентифікації. Щоб можна було динамічно змінювати метод аутентифікації в залежності від поточних ризиків атак.

Методи. Метод полягає в розробці математичної моделі і її симуляції. Потім модель спирається на сукупність сильних сторін окремих факторів аутентифікації. Для визначення параметрів моделі використовується механізм на основі ризику.

Результати. У статті продемонстровано результати моделювання за допомогою широко використовуваних засобів аутентифікації: пароля, одноразового пароля на основі апаратних засобів, відбитків пальця, зовнішньої аутентифікації та комбінації цих методів. Результати показали, що використання цієї математичної моделі полегшує моделювання використання ресурсів аутентифікації.

Висновки. Запропонована модель дозволяє легко моделювати різні ситуації з безпекою. В реальній ситуації параметри моделі потрібно буде уточнити в рамках оцінки зворотного зв'язку встановлених інцидентів з безпекою.

КЛЮЧОВІ СЛОВА: аутентифікація, багатофакторна автентифікація, аутентифікація на основі ризику, аутентифікація фактора omni, система виявлення шахрайства, пароль, цифровий відбиток

УДК 004.738

МУЛЬТИ-ФАКТОРНОЕ МОДЕЛИРОВАНИЕ АУТЕНТИФИКАЦИИ

Досталек Л. – магистр, аспирант кафедры компьютерных наук и инженерии, Университет Западной Богемии в Пльзне, Чехия.

Шафарик Й. – канд. техн. наук, профессор, профессор кафедры компьютерных наук и инженерии, Университет Западной Богемии в Пльзне, Чехия.

АННОТАЦИЯ

Актуальность. В настоящее время, учреждения и компании сталкиваются с массовыми кибератаками. Атаки всегда сосредоточены на некоторой слабости аутентификации, которая является частью конкретного протокола аутентификации. В случае нападения необходимо гибко реагировать на ослабление механизмов аутентификации. В случае нападения необходимо быстро определить пострадавший фактор аутентификации и временно ослабить его значение. Впоследствии можно обнаружить пораженную слабость и ослабить значение лишь алгоритмов, проявляющих эту слабость. Алгоритмы,

DOI 10.15588/1607-3274-2020-2-11

которые не проявляют такой слабости, следует оставить без изменений. В этой работе представлена математическая модель аутентификации. Быстро изменяя параметры модели, мы можем гибко адаптировать использование средств аутентификации к ситуации.

Цель работы – предложить метод позволяющий количественно оценить силу (качество) аутентификации. Чтобы можно было динамически менять метод аутентификации в зависимости от текущих рисков атак.

Методы. Метод заключается в разработке математической модели и ее симуляции. Затем модель опирается на совокупность сильных сторон отдельных фактором аутентификации. Для определения параметров модели используется механизм на основе риска.

Результаты. В статье продемонстрированы результаты моделирования с помощью широко используемых средств аутентификации: пароля, одноразового пароля на основе аппаратных средств, отпечатков пальца, внешней аутентификации и комбинации этих методов. Результаты показали, что использование этой математической модели облегчает моделирование использования ресурсов аутентификации.

Выводы. Предложенная модель позволяет легко моделировать различные ситуации с безопасностью. В реальной ситуации параметры модели нужно будет уточнить в рамках оценки обратной связи установленных инцидентов с безопасностью.

КЛЮЧЕВЫЕ СЛОВА: аутентификация, многофакторная аутентификация, аутентификация на основе рисков, многофакторная аутентификация, система обнаружения мошенничества, пароль, цифровой отпечаток.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Dostálek L. Omnifactor Authentication/ L. Dostálek I. Dostálková // Advanced Computer Information Technologies: International Conference ACIT 2018, Ceske Budejovice, 1–3 June 2018: proceedings. – Ternopil : TNEU, 2018. – P. 228–231.
2. Alaca F. Device fingerprinting for augmenting web authentication: classification and analysis of methods / F. Alaca, P. C. Oorschot // Computer Security Applications: the 32nd Annual Conference ACSAC '16, Los Angeles, California, USA, 2016: proceedings. – Los Angeles, California, USA, 2016 – P. 289–301. DOI: https://doi.org/10.1145/2991079.2991091
3. Yang Z. Effective Mobile Web User Fingerprinting via Motion Sensors / Z. Yang, R. Zhao, C. Yue// Trust, Security And Privacy In Computing And Communications: 17th IEEE International Conference / Big Data Science And Engineering: 12th IEEE International Conference, 1–3 Aug. 2018: proceedings. – New York, NY, USA, 2018 – P. 1398–1405. DOI: 10.1109/TrustCom/BigDataSE.2018.00194
4. Arya V. Does digital footprint act as a digital asset? – Enhancing brand experience through remarketing / V. Arya, D. Sethi, J. Paul // International Journal of Information Management. – 2019. – Vol. 49. – P. 142–156. https://doi.org/10.1016/j.ijinfomgt.2019.03.013
5. Hinds J. Human and Computer Personality Prediction from Digital Footprints / J. Hinds, A. Joinson // Current Directions in Psychological Science. – 2019. – Vol. 28, Issue 2. – P. 204–211. https://doi.org/10.1177%2F0963721419827849
6. Pat. US7,908,645B2 US, H04L63/20, System and Method for Fraud Monitoring, Detection, and Tired User Authentication / T. E. Varghese, J. B. Fisher, S. L. Harris, D. D. Boseo (US), applicant Oracle International Corporation. – № 11/412,997; 28.04.2006; 14.12.2006. – 51 p.
7. Fraud detection for E-commerce transactions by employing a prudential Multiple Consensus model / [S. Carta, G. Fenu, D. R. Recupero, R. Saia] // Journal of Information Security and Applications. – 2019. – Vol. 46. – P. 13–22.
8. Information technology – Security techniques – Information security risk management: ISO/IEC 27005:2018. – [Effective from 2018-07]. – 2018. – 56p.
9. Dostálek L. Multi-Factor Authentication Modeling / L. Dostálek // Advanced Computer Information Technologies: 9th International Conference ACIT’2019, Ceske Budejovice, Czech Republic, 5–7 June 2019: proceedings. – Ternopil : TNEU, 2019. – P. 443–446. DOI: 10.1109/ACITT.2019.8780068.
10. Vijaya C. J. Authentication and authorization mechanism for cloud security / C. J. Vijaya, N. Challa, S. K. Pasupuletti // International Journal of Engineering and Advanced Technology. – 2019. – Volume 8, Issue 6, August. – P. 2072–2078, E-ISSN:2249-8958

DOI 10.15588/1607-3274-2020-2-11