Proceedings of the Federated Conference on Computer Science and Information Systems pp. 1021–1030
DOI: 10.15439/2016F219
ACSIS, Vol. 8. ISSN 2300-5963

A new authentication management model oriented on user's experience

Mariusz Sepczuk , Zbigniew Kotulski,
Institute of Telecommunications
Warsaw University of Technology
Warsaw, Poland
Email: {msepczuk, zkotulsk} @tele.pw.edu.pl

***Abstract*— Authenticating users connecting to online services, social networks or m-banking became an indispensable element of our everyday life. Reliable authentication is a foundation of security of Internet services but, on the other hand, also a source of users' frustration due to possible account blocking in case of three fails. In this paper we propose a model of authentication service management which helps in keeping a balance between the authentication security level and positive users' perception of this procedure. The proposed procedure allows a user more than three attempts of authentication by switching after two failures to a more secure authentication protocol keeping a balance between QoP and QoE measures. Finally, the procedure determines an optimal path of authentication using a decision tree algorithm.**

***Index Terms*— authentication, Quality of Experience, Quality of Protection.**

I. INTRODUCTION

Diversity of Internet services at the present time grows faster and faster. In particular, the variety of manners in which the services are provided, from a wired environment (e.g., LAN) to a wireless environment (e.g. WiFi, mobile environment), is observed. Many users become more and more demanding about services' usability. Thus, any services, especially newly designed, should be developed taking into account users' satisfaction factor.

One of the main issues in all Internet services is security protection. Nowadays, there are few user- friendly and at the same time secure services. It is well known that for most services the high level of protection makes their usability is declined. So, it is important to find a balance between security and usability of a service. Of course, that idea depends on kind of a protection mechanism which is considered. Examples of such security mechanisms are authentication solutions. The authentication is an act of reliable entity identification. Within this process two problems can be considered: a choice of the specific authentication solution and its influence on user's behavior. The choice of the proper identification mechanism isnot a simple problem, because many factors can have a significant impact on it. Even if such a mechanism is selected, in most cases it is not considered how a person feels using it. Therefore, an appropriate authentication solution should provide both an adequate security level and sufficient users' satisfaction.

In this paper we propose a service model which can be used to proper management of the authentication mechanisms based on users' satisfaction.

The rest of the paper is organized as follows: Section 2 presents a connection between QoP and QoE measures characterizing Internet services. Section 3 briefly discuses an impact of security context and contextual data on security management while Section 4 presents basic known results on contextual security and user-friendly authentication mechanisms. .Section 5 contains main theoretical result of the paper which is an authentication management model oriented on user's experience. Finally, Section 6 presents results of a simulation which confirms correctness of a created model and Section 7 concludes the paper and outlines the future work.

II. RELATION BETWEEN QOS, QOE AND QOP

In Internet services, to measure Quality of Service (QoS) [1] many parameters like jitter, network latency, throughput, etc. are used. Based on their value a service and a network parameters should be correctly modify to ensure the best quality. However, not always changing a QoS parameter is enough to provide a good quality service. Sometimes to provide high quality of a service not all parameters should have the best values. In most cases it is expensive to set the best values of QoS parameters. Thus, investigations concerning users' experience were conducted. As a result of the research a Quality of Experience (QoE) factor was designed [2, 3]. This implies that QoS parameters should be set based on a users' QoE value [4, 5].

In the area of security the Quality of Protection (QoP) measure is a counterpart of QoS [6, 7]. The term defines a minimum protection level that should be provided to a secure Internet service. For example, it is obvious that different level of protection ensures an authentication mechanism which used a hash function SHA-1 than those with a hash function SHA-2/256 [8]. So, it is natural to measure a level of protection which is required. But, as it is for QoS, not always a security mechanism applied meets users' requirements. Sometimes the mechanism is too

978-83-60810-90-3/$25.00

difficult to use (e.g., a multi-factor authentication can be a barrier for elder people), sometimes it is too annoying (e.g., a continuous request for fingerprinting due to a device read/scan problems).

To summarize above considerations, the relationship between QoS, QoP and QoE can be presented in a form of the graph (see Fig 1). The QoS parameter has an impact on security services (a security level) and at the same time on users' satisfaction. Once again, a proper security mechanism should be provided with respect to a user's expectations.

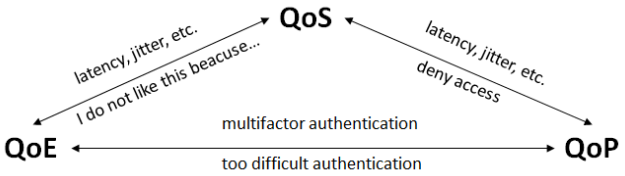

Figure 1. Relationship between QoS, QoP and QoE

An open problem is to answer a question which mechanism should be provided in particular conditions. For this issue the solution can be the idea of context-based systems in which a state of the system is dynamically changed with respect of environmental conditions.

III. Security context

The term "context" concerns all data which can be used to adapt state of a system to particular conditions. They come from many sources [9].There are many descriptions about context. In [10] Schilit et. al. show context-aware systems as systems able to adapt to dynamically and continuously changing GPS coordinates , type of devices, people relations and time. The author describes three features of context data: where you are?, with whom you are?, what is your neighborhood? Furthermore, he emphases that contextual information is not only a localization, but also other useful information. Recently this definition had been used by many authors. In general they claim that contextual data are data which are answers on a question that starts with: Who?, Where?, What?, When?. Beside context-aware system, description of the context-aware application can be found in [11]. More universal definition was proposed by Wrona and Gomez [12]. According to them the contextual data are information which can describe a state of an entity. This definition is better than the previous one because it includes all data which can be contextual information.

Some contextual data have common features. For example, day, part of a year and day of birth apply to determine the time while GPS coordinates, the UK and the Earth describe a localization. For this reason it is naturally to divide contextual data into categories. Two context categories were are already defined: time and position. Beside these, many more exist like: access device, operating systems, environment, neighborhood, etc.

All contextual information can be divided in three classification groups: storage of context, retrieval of context and its dynamism. First group includes all aspects of store data (in database, in Hidden Markov Model, in file, etc.). Second group describe different aspects of data retrieval like its history, presentation, the way in which was gathered, etc. The last third group consists data connected with a specific environment- some environment could be dynamically changed over time and some could be more static- every information changed very rarely or not changed at all.

As it was shown in the literature (see e.g., [13, 14, 15]) contextual information can be used to improve Internet systems work. Using contextual data, QoP and QoE measures combination cause that a model of providing the best authentication mechanism adequate for specific requirements can be created.

IV. User authentication and Quality of Experience: related works

As mentioned earlier, not many works apply to problem of providing an appropriate authentication mechanism based on user's context and respecting the user's QoE. Security solutions which include contextual data aspects are more common. Several approaches for the context security have been described in [16, 17, 18, 19]. The authors in their papers present an idea how contextual information can be used in an authentication mechanism, but they do not consider user's Quality of Experience. Another example of using contextual data in security is access control approach. Based on sensitivity or importance of data (e.g. patient health history, personal data, etc.), proper access to them should be provided to avoid information leakage. This idea is shown in [20, 21, 22, 23]. However, the aspects of security should be considered as well as user's satisfaction. In most cases it is difficult to obtain an answer to the question which security features have impact on user's experience. In [24] the authors present the results of a survey of over 300 users to determine their understanding of the security feature in selected applications. The experiment includes some areas of difficulty with many security features showing usability challenges for users. Similar considerations includes the paper [25]. Based on conclusions from [24, 25] was created a few papers which apply to experiments of balancing QoE and QoP. In [26, 27] is described provisioning of QoE and QoP in Mobile Networks and Wireless Networks. Authors focus on ensuring an appropriate level of QoE and QoE of cryptographic algorithms used in a mobile environment. The paper [28] shows long – term QoP in mobile networks with QoE aspects, too. More experimental results can be found in [29]. The paper contains research about impact of an authentications mechanism on users perceive logins. Computed exponential QoE-QoP relationship can be served to assessing used identification mechanism in the domain of user acceptability. The extension of these research and more detailed description can be found in [30, 31]. Based on [29] was created an experiment shown in [32]. The author tries to find QoE – QoP dependence in popular SaaS cloud products. A similar approach, but with mobile devices, is shown in [33], where security barriers survey was described.

Other, more holistic idea of connection security and user experience can be found in [34]. The paper shows a framework of

criteria for the evaluation of authentication schemes in IMS, focus on security, user-friendliness and simplicity. Very interesting description contains [35] where authors explain how contextual information can be used to provide secure and user oriented mechanisms. The paper [36] is an example of using the framework from the paper [35] for constructing an adaptable authentication protocol.

V. Authentication Model Using User's Context and QoE

A described solution is an example of a model which helps in authentication mechanisms management. The model was created to provide a correct authentication mechanism based on user's context (e.g. position, time, neighborhood, etc.) and on the knowledge about user's experience in using a particular authentication service. One of the most important elements of the model is a table which contains a list of authentication mechanisms (A_1,A_2,…,A_n) and their QoP (QoP_1,QoP_2,…,QoP_n) and QoE (QoE_1,QoE_2,…,QoE_n) measures (see TABLE I). The values of such parameters (measures) are usually based on experts' knowledge and data obtained from experiments. The table is used to select the best authentication mechanism from many possible choices.

TABLE I
ASSIGNMENT OF AUTHENTICATION MECHANISMS AND THEIR QOP AND QOE VALUES

LP	Kind of mechanism	QoP	QoE
1	A_1	QoP_1	QoE_1
2	A_2	QoP_2	QoE_2
3	A_3	QoP_3	QoE_3
…	…	…	…
n	A_n	QoP_n	QoE_n

A user who wants to use a service at first must authenticate himself. Based on current user's context the required minimal value of Quality of Protection level is calculated according to formula (1):

$$f(c_1, c_2, c_3, \ldots, c_m) = QoP_c \tag{1}$$

where c_1,c_2,…,c_m are context factors.

Having the boundary QoP_c value it is possible to select some authentication mechanisms for which the QoP value is greater than or equal to QoP_c. The best authentication mechanism can be chosen using a decision tree structure (see Fig. 2). The tree is spanned on j states. Each state represents a situation in which a user tries to authenticate himself with a particular authentication protocol. In every state the user has two trials to identify himself with a selected protocol (of course, twice means that first trial was failed and now is a second trial). In the third trial, when the first and second trials were incorrect, he or she can still use the same protocol or, if it is possible, change an authentication protocol to some more convenient in a specific situation. If he or she decides to change the protocol, the new one is with a higher value of OoP. The required higher value of QoP implicates less probability of a successful attack in three trials of the new protocol than in a case of a single try in the previous one. A user can choose a new authentication protocol option until the cumulative value of QoP in a current state does not achieve the boundary value QoP_c.

The main goal of created model is to choose the best path of the tree. The best path means a scenario where a user uses the last authentication protocol in the state j and he finally authenticates correctly with the highest probability. Moreover, the path should contain the authentication protocols which are relatively simple, secure and at the same time with the high value of the QoE measure. A choice of this path could be made by calculations based on a decision tree algorithm. In the next paragraph we will describe the probability of a successful authentication in every branch of the decision tree.

As it shown in Figure2, in an authentication decision tree there are two types of states: state 1 without changing an authentication protocol (but with three possible trials of the same protocol) and the states from 2 to n where a user changes this protocol (after two trials of the same protocol he or she tries with a new one in the third trial). Furthermore, every trial of an authentication protocol can be successful; the event R_{ij} means that in state i (i=2…n), in its step j (j=1,2,3) an authentication is right or successful , the event F_{ij} means that in state i, in its step j the authentication fails. Moreover, the event B_i was defined as correct authentication in state i after using all options of a path. So, for state 1 the probability of correct authentication according to (2) is equal:

$$\begin{aligned} P(B_1) = {} & P(R_{11}) + P(R_{12} \mid F_{11})P(F_{11}) + \\ & P(R_{13} \mid F_{11} \cap F_{12})P(F_{11} \cap F_{12}) \end{aligned} \tag{2}$$

The state 2 and next states are different from state 1, thus, for state 2 the probability of correct authentication according to (3) is equal:

$$\begin{aligned} P(B_2) = {} & P(R_{21} \mid F_{11} \cap F_{12})P(F_{11} \cap F_{12}) + \\ & P(R_{22} \mid F_{11} \cap F_{12} \cap F_{21})P(F_{11} \cap F_{12} \cap F_{21}) + \\ & P(R_{23} \mid F_{11} \cap F_{12} \cap F_{21} \cap F_{22})P(F_{11} \cap F_{12} \cap F_{21} \cap F_{22}) \end{aligned} \tag{3}$$

Analogously, it is possible to calculate the probability of correct authentication formula for each states from 2 to n. A general formula for the states from 2 to n is equal:

$$\begin{aligned} P(B_n) = {} & P\left(R_{n1} \mid \left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right)\right) P\left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right) + \\ & P\left(R_{n2} \mid \left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right) \cap F_{n1}\right) P\left(\left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right) \cap F_{n1}\right) + \\ & P\left(R_{n2} \mid \left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right) \cap F_{n1} \cap F_{n2}\right) P\left(\left(\bigcap_{j=1}^{n-1} F_{j1} \cap F_{j2}\right) \cap F_{n1} \cap F_{n2}\right) \end{aligned} \tag{4}$$

Finally, a formula for the probability of correct authentication in a decision tree is equal according to (5):

$$P(B_n)=\begin{cases} P(R_{11})+P(R_{12}\mid F_{11})P(F_{11})+P(R_{13}\mid F_{11}\cap F_{12})P(F_{11}\cap F_{12}) & ,for \quad n=1 \\ P\left(R_{n1}\mid\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)\right)P\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)+P\left(R_{n2}\mid\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)\cap F_{n1}\right)\cdot & \\ P\left(\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)\cap F_{n1}\right)+P\left(R_{n3}\mid\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)\cap F_{n1}\cap F_{n2}\right)P\left(\left(\bigcap_{j=1}^{n-1}F_{j1}\cap F_{j2}\right)\cap F_{n1}\cap F_{n2}\right) & ,for \quad n=2,\ldots,n \end{cases} \tag{5}$$

TABLE II
EVENTS AND THEIR IMPACT ON QOE AND QOP MEASURES

	QoE			QoP	
	Description	Parameter	Value	Description	Parameter
Increase	A user has still possibility of authentication using the same or a new mechanism	α	≈0,15	An authentication mechanism was changed	QoP_j
Increase	A user finally authenticate himself	β	≈0,25		
Decrease	With every user try his or her satisfaction is lower	γ	≈0,1	First or second trial was failed	$\frac{1}{\lvert t_j\rvert}$

To obtain the best authentication path it is necessary to calculate the probability of correct authentication for every branch of the tree in a state number n (we denote it as $P(B_{nm})$ where m means a number of the branch). From the set of received probabilities the maximal value is selected ($\max\{P(B_{n1}), P(B_{n2}), P(B_{n3}),\ldots, P(B_{nm})\}$) and this value indicates a path with authentication mechanisms which should be used to deliver proper levels of protection (QoP) and user's satisfaction (QoE).

Beside the probability of a successful authentication, the level of QoP and QoE measures for every branch of the tree should be calculated. These two values define together a new parameter called Quality of User Security Service (QoUSS). Usually in literature information about parameter QoSS (Quality of Security Services) can be found. This factor describes security based on QoS of an Internet service [37, 38]. The QoUSS measure includes information about both the security level and, what is important, the satisfaction level of a used service; it is defined by a function:

$$f(QoP, QoE) = QoUSS \tag{6}$$

The argument QoE in that formula means final user satisfaction after correct authentication in a last state and QoP means the resultant level of protection in the final state.

Before we define the expressions for calculating QoE and QoP measures suitable in our model, let us describe example cases which can have impact on these two values. The TABLE II includes events which affect increase or decrease of the QoUSS arguments.

We postulate that the values of parameters moderating QoP and QoE included in TABLE II should be small, because they must not impact a resultant value of the measures. They are considered as correction parameters, so we assume $\alpha, \beta, \gamma \in (0,1)$. In TABLE II we proposed some intuitively assumed values of these parameters to reflect users' emotions connected with successes and fails of their authentication. More realistic parameters should be dedicated to specific authentication mechanisms and they must be obtained from gathering experimental data. Moreover, the value QoP_j is a minimal protection level of a new authentication protocol and $|t_j|$ is the number of all possible trials of the authentication protocol in step number j.
Thus, we propose the QoP formula as:

$$QoP_{jFIN} = QoP\left(1-\frac{1}{|t_j|-1}\right). \tag{7}$$

The proposed formula for QoE is more complicated, so it will be briefly described.
Again, like in the case of calculating the probability of a successful authentication, all states can be divided on two QoE types:

- The first state when an user authenticates himself,
- The second and next states when an user authenticates himself.

We propose a general formula of MOS dependency in an exponential form:

$$QoE = A\cdot\exp\{Z\} \tag{8}$$

where A is a constant value allowing tune the model to users' behavior, e.g., $A\in(0{,}01;1)$.

Such a shape of this function is to provide adequate sensitivity of the measure in critical areas of minimal and maximal scorings. The argument Z depends on a state in a decision tree, and the scaling constant A is determined by the MOS scale (which is from 1 to 5). Each authentication protocol has a particular QoE value. For the first failed try a user can be a little confused that he does not authenticate himself (the QoE decreases with γ_1) and at the same time the user feels good that he or she can still try with next attempt (the QoE value increases with α_1). For the second failed try user is more confused (decrease with

γ_2) but still can try authenticate himself (increase with α_2). Finally, a user authenticates himself so his satisfaction increases with the value (β).
In most cases MOS dependency has an exponential distribution, so in the first state final QoE value is equal:

$$QoE_{jFIN=1} = \begin{cases} 1 & ,if\ A \cdot \exp\{Z\} \le 1 \\ A \cdot \exp\{Z\} & ,if\ 1 < A \cdot \exp\{Z\} < 5 \\ 5 & ,if\ A \cdot \exp\{Z\} \ge 5 \end{cases} \quad (9)$$

where $Z = QoE_1 - \gamma_1 - \gamma_2 + \alpha_1 + \alpha_2 + \beta$

For the second state (and each next one) the value of QoE depends on QoE value from the previous state. QoE value on the beginning of a new state, which is connected with the previous is equal:

$$QoE_{j-1FIN} = \begin{cases} 1 & ,if\ A \cdot \exp\{Z\} \le 1 \\ A \cdot \exp\{Z\} & ,if\ 1 < A \cdot \exp\{Z\} < 5 \\ 5 & ,if\ A \cdot \exp\{Z\} \ge 5 \end{cases} \quad (10)$$

where $Z = QoE_1 - \gamma_1 - \gamma_2 + \alpha_1 + \alpha_2 + \alpha_3$

The value of α_3 is reflects the result of changing the authentication protocol. Basically founding connection between two values of QoE and calculation one average value is a difficult issue. Thus, reasonable is to assume the worst case in which choosing value is lesser. In presented case the lesser value is chosen between a value from the previous state and the QoE value for the present authentication protocol (for the present state):

$$QoE_j = \min\{QoE_{j-1FIN}, QoE_{jFIN}\} \quad (11)$$

For such a value of QoE calculations are performed based on formula (8) in case of an authentication. When the user finally do not authenticate correctly, his/her QoE decrees to 0 (but with flow of time this value can grow because the user thinks about this situation and agrees that this mechanism is secure and protects him against crackers).

Finally, for each branch of the tree the following 3-tuple was calculated: **$(P(B_n), QoE_{FINpath}, QoP_{FINpath})$**. Probability of choosing particular path includes QoE and QoP values. But it may be that paths have values like in TABLE II.

TABLE III
EXAMPLE OF RESULTS OF THE DECISION TREE ALGORITHM

Path number	1	2	3	4
QoE	3	3,5	4,5	3
QoP	3	4,5	3,5	4
Probability	0,5	0.9	0,7	0,6

It would seem that the path number 2 is the best one when considering the probability. However it is not so obvious. The path number 3 has a higher value of QoE, but a lesser value of QoP. Due to this fact there is need to use multi-objective optimization to choose the best path.
Let us assume that all results from the decision tree algorithm are in TABLE IV.

TABLE IV
ALL RESULTS FROM THE DECISION TREE ALGORITHM

Path number	1	2	3	4	…	n	**Weight**
QoE	qoe_1	qoe_2	qoe_3	qoe_4	…	qoe_n	$\mathbf{w_1}$
QoP	qop_1	qop_2	qop_3	qop_4	…	qop_n	$\mathbf{w_2}$
Probability	p_1	p_2	p_3	p_4	…	p_n	$\mathbf{w_3}$

To choose which path is the best weight sum method should be used. In general below conditions must met:

Maximize: $f(u) = \sum_{i=1}^{n} w_j \cdot K_i(u)$

Subject to: $u \in U$,
where the weights w_i, i=1,…,n corresponding to objective function satisfy the following conditions:

$$\sum_{i=1}^{n} w_1 = 1, \quad w_i \ge 0, \quad i = 1,\ldots,n,$$

and $K_i(u)$ is the objective function and U is feasible design space.
In general the maximized formula must be satisfied:

$$u_k \succ u_l \Leftrightarrow \sum_{i=1}^{n} w_i \cdot K_i(u_k) > \sum_{i=1}^{n} w_i \cdot K_i(u_l)$$

It means that decision u_k is better than decision u_l when sum of multiplications of weight and objective function of decision u_k is greater than for the decision u_l.

In presented case the function f(u) for each path is presented in TABLE V

TABLE V
VALUE OF FUNCTION F(U) IN MULTI –OBJECTIVE OPTIMIZATION

Path number	1	2	3	4	…	n	**Weight**
QoE	qoe_1	qoe_2	qoe_3	qoe_4	…	qoe_n	$\mathbf{w_1}$
QoP	qop_1	qop_2	qop_3	qop_4	…	qop_n	$\mathbf{w_2}$
Probability	p_1	p_2	p_3	p_4	…	p_n	$\mathbf{w_3}$
f(u)	$qoe_1 \cdot w_1 + qop_1 \cdot w_2 + p_1 \cdot w_3$	$qoe_2 \cdot w_2 + qop_2 \cdot w_2 + p_2 \cdot w_3$	$qoe_3 \cdot w_1 + qop_3 \cdot w_2 + p_3 \cdot w_3$	$qoe_4 \cdot w_1 + qop_4 \cdot w_2 + p_4 \cdot w_3$		$qoe_n \cdot w_1 + qop_n \cdot w_2 + p_n \cdot w_3$	

Of course to perform optimization values of should be normalized. What is also important that calculation are made with assumption that the most important should be path with the highest QoE value than path with QoP value and a finally probability of path. It means that $w_1 > w_2 > w_3$.
In considered example f(u) has the following values (see TABLE VI):

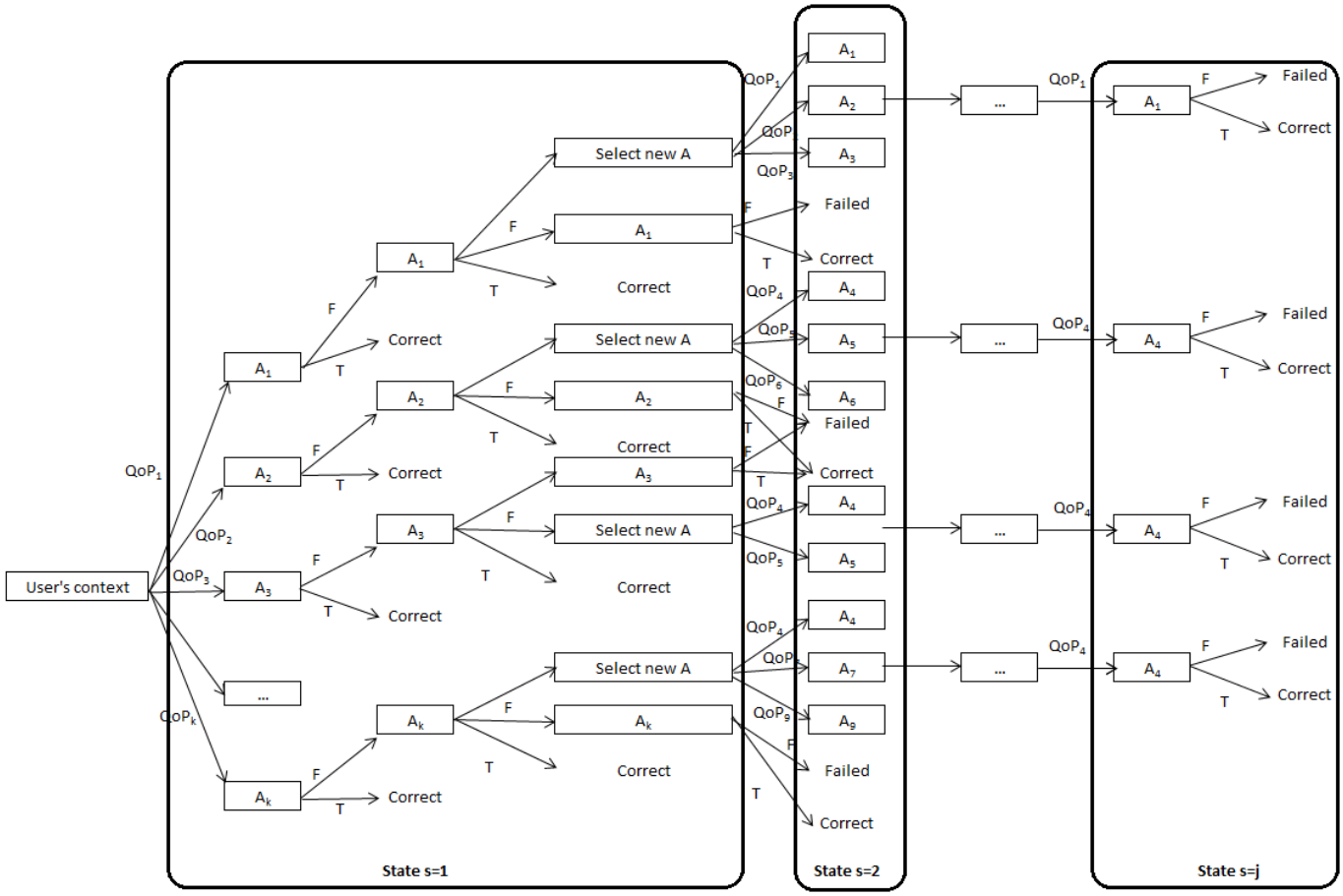

Figure 2. A decision tree for the authentication mechanism

TABLE VI
THE VALUE OF FUNCTION F(U) IN THE CONSIDERED EXAMPLE

Path number	1	**2**	**3**	4	**Weight**
QoE	0,6	**0,7**	0,9	0,6	**0,45**
QoP	0,6	**0,9**	0,7	0,8	**0,35**
Probability	0,5	**0,9**	0,7	0,6	**0,2**
f(u)	0,58	**0,81**	0,79	0,67	

Based on TABLE VI, the best path with authentication mechanism is the second one, but a few more than third path.

VI. Discussion

Now some facts about α, β, γ impact on the formula (7) will be considered. The discussion assumes two scenarios:

- A user correctly authenticates himself in the third step in stage number 1 (Scenario 1),
- A user correctly authenticates himself in the third step in stage number 2 (Scenario 2).

For these scenarios TABLES VIA, VIB, VIC (Scenario 1), VIIA, VIIB, VIIIA, VIIIB, VIIIC (Scenario 2) and corresponding to them charts were created. In Scenario 1 and Scenario 2 we assume the factor A=0,075. Moreover, if the value of QoE_{FIN} after calculations is greater than 5, automatically it is corrected to 5.

TABLE VIA
PARAMETERS FOR SCENARIO 1 – INCREASE OF Γ

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,1	3,56
3,5	0,15	0,16	0,25	0,2	0,25	2,77
3,5	0,15	0,16	0,25	0,25	0,3	2,51
3,5	0,15	0,16	0,25	0,3	0,33	2,32
3,5	0,15	0,16	0,25	0,35	0,4	2,05

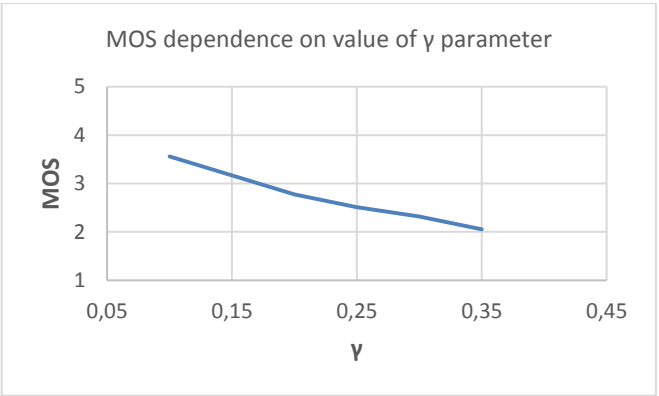

Figure 3. MOS dependence on value of γ factor in Scenario 1

TABLE VIB
PARAMETERS FOR SCENARIO 1 – INCREASE OF A

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,15	3,39
3,5	0,2	0,22	0,25	0,1	0,15	3,78
3,5	0,25	0,3	0,25	0,1	0,15	4,30
3,5	0,31	0,35	0,25	0,1	0,15	4,81
3,5	0,35	0,4	0,25	0,1	0,15	5,00

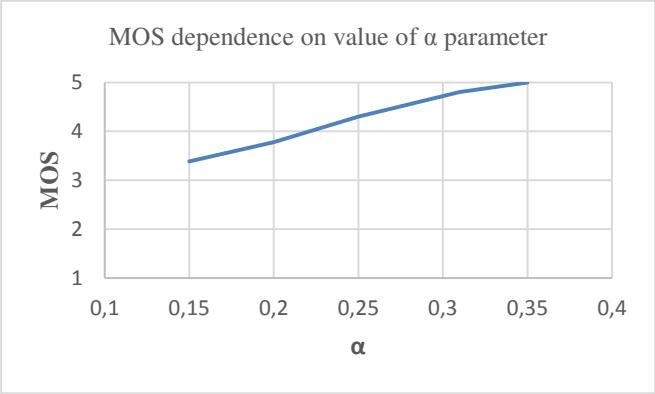

Figure 4. MOS dependence on value of α factor in Scenario 1

TABLE VIC
PARAMETERS FOR SCENARIO 1 – INCREASE OF B

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,15	3,39
3,5	0,15	0,16	0,3	0,1	0,15	3,56
3,5	0,15	0,16	0,35	0,1	0,15	3,74
3,5	0,15	0,16	0,4	0,1	0,15	3,93
3,5	0,15	0,16	0,45	0,1	0,15	4,14

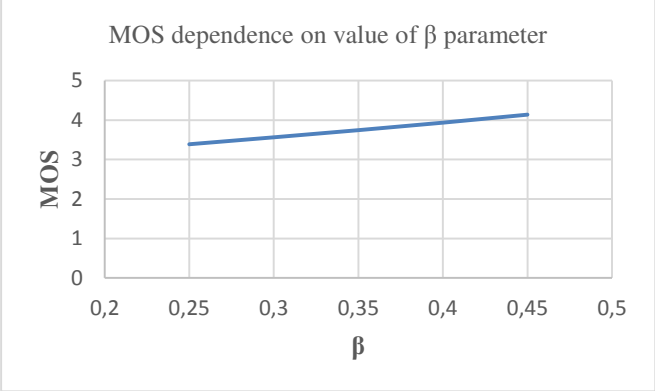

Figure 5. MOS dependence on value of β factor in Scenario 1

Based on Scenario 1 with a correct authentication in third step increase of α, β, γ parameters will be considered with their impact on a final QoE value. Figure 3 shows a situation in which γ increases and QoE value decreases. According to formula (7) it is a proper behavior. The γ factor is a parameter of QoE, which informs about decreeing of user's satisfaction. The greater factor is, the worse final QoE value is. Figure 4 shows the case in which α parameter increases. As it was shown in Figure 4, the greater α values are, the greater final QoE value is. But, wrong choice of α parameters results in a too high final value of QoE: for greater α the value of QoE is greater than 5 (but of course in MOS scale it will be corrected to maximum 5).Thus, α parameter should be determined on a proper, not too high level. Finally, Figure 5 presents β parameter impact on the final QoE value. As it was shown, QoE value increases with β increasing. And it is a proper situation, because β is a factor which value describes user's satisfaction when he/she correctly authenticates him/herself. Moreover, Figure 5 shows that β has not got such an impact on QoE as α has.

Comparing all these three factors we can notice that a significant influence has the α parameter. As a result the final QoE value can be overestimated.

TABLE VIIA
PARAMETERS FOR SCENARIO 2 – PART 1

QoE_1	α_1	α_2	α_3	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,17	0,1	0,15	3,13
3,5	0,15	0,16	0,17	0,2	0,25	2,56
3,5	0,15	0,16	0,17	0,25	0,3	2,32
3,5	0,15	0,16	0,17	0,3	0,33	2,14
3,5	0,15	0,16	0,17	0,35	0,4	1,90

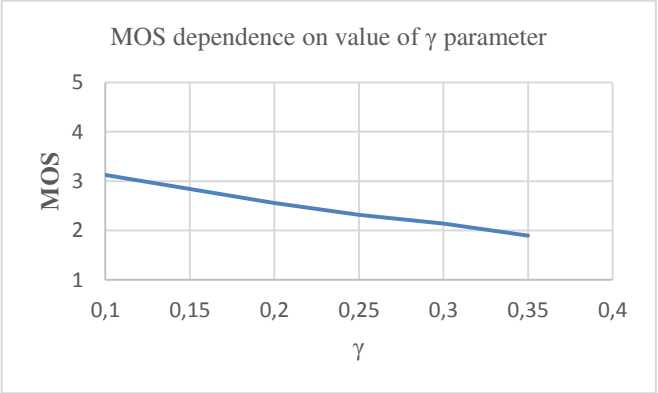

Figure 6. MOS dependence on value of γ factor in Scenario 2 - part 1

TABLE VIIB
PARAMETERS FOR SCENARIO 2 – PART 1

QoE_2	α_1	α_2	β	γ_1	γ_2	QoE_{2FIN}
3,5	0,15	0,16	0,17	0,1	0,15	3,13
3,5	0,2	0,22	0,24	0,1	0,15	3,74
3,5	0,25	0,3	0,33	0,1	0,15	4,66
3,5	0,31	0,35	0,37	0,1	0,15	5,00
3,5	0,35	0,4	0,43	0,1	0,15	5,00

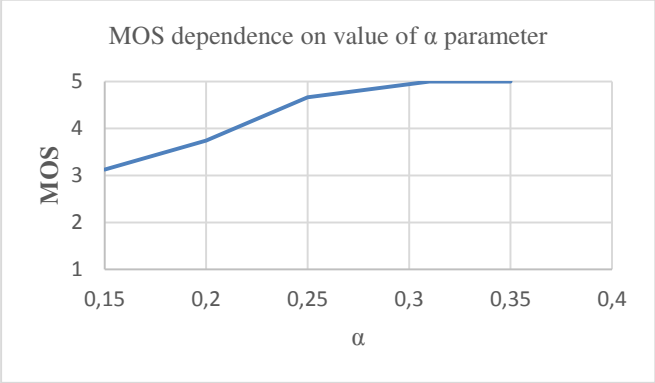

Figure 7. MOS dependence on value of α factor in Scenario 2 - part 1

Considering part 1 of Scenario 2 it can be noticed that α and β factors have similar tendency like in the Scenario 1 – an increase of γ results in decrease of QoE and an increase of α results in too fast QoE increase.

TABLE VIIIA
PARAMETERS FOR SCENARIO 1 – PART 2: INCREASE OF Γ

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,15	3,39
3,5	0,15	0,16	0,25	0,2	0,25	2,77
3,5	0,15	0,16	0,25	0,25	0,3	2,51
3,5	0,15	0,16	0,25	0,3	0,33	2,32
3,5	0,15	0,16	0,25	0,35	0,4	2,05

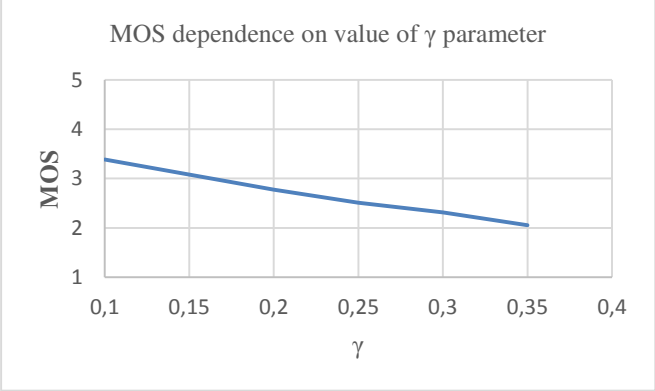

Figure 8. MOS dependence on value of γ factor in Scenario 2 - part 2

TABLE VIIIB
PARAMETERS FOR SCENARIO 1 – PART 2: INCREASE OF A

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,15	3,39
3,5	0,2	0,22	0,25	0,1	0,15	3,78
3,5	0,25	0,3	0,25	0,1	0,15	4,30
3,5	0,31	0,35	0,25	0,1	0,15	4,81
3,5	0,35	0,4	0,25	0,1	0,15	5,00

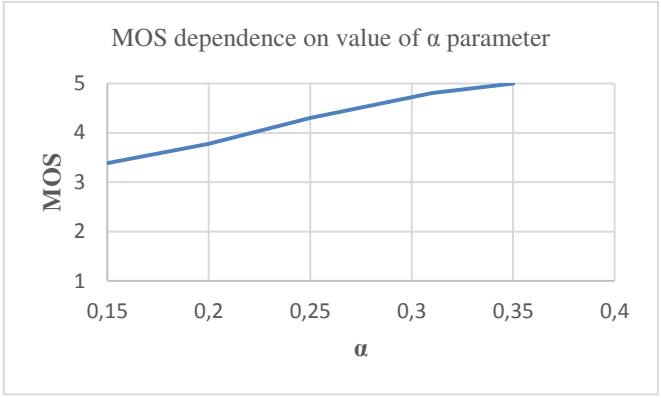

Figure 9. MOS dependence on value of α factor in Scenario 2- part 2

TABLE VIIIC
PARAMETERS FOR SCENARIO 1 – PART 2: INCREASE OF B

QoE_1	α_1	α_2	β	γ_1	γ_2	QoE_{1FIN}
3,5	0,15	0,16	0,25	0,1	0,15	2,89
3,5	0,15	0,16	0,3	0,1	0,15	3,03
3,5	0,15	0,16	0,35	0,1	0,15	3,19
3,5	0,15	0,16	0,4	0,1	0,15	3,35
3,5	0,15	0,16	0,45	0,1	0,15	3,52

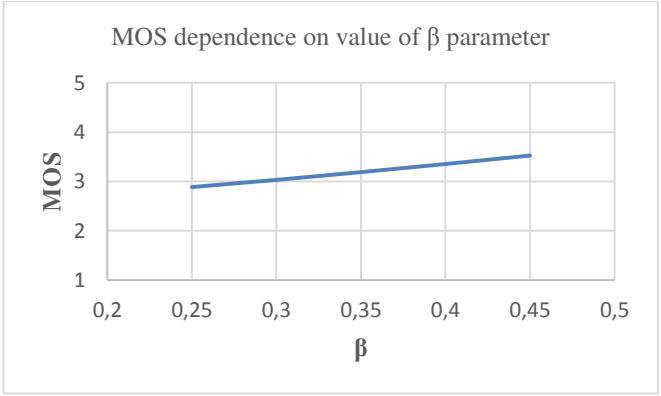

Figure 10. MOS dependence on value of β factor in Scenario 2 - part 2

Considering part 2 of Scenario 2 we can notice that it is similar to Scenario 1 – α parameter has a meaningful impact on the final QoE value.

VI. Conclusions and Future Work

In this paper a model of selecting the best authentication mechanism has been proposed. The model consists of two stages. The first stage constructs a decision tree algorithm, which is used to calculate three parameters characterizing the authentication: a probability of choosing particular path describing the steps of authentication, a final QoP value and a final QoE value. The second stage concerns multi-objective optimization of the measures established in the first stage. Based on a weighted sum method applied to QoP and QoE measures for the authentication mechanism the best path is chosen. Moreover, a discussion about an impact of QoE parameters on a final value of QoE was

conducted. The assumptive final QoP and QoE formulas fulfill requirements applied to acceptable values. In spite of all, experiments which verify created formulas should be performed.

To illustrate the results a simple numerical example has been presented. In our future work the research will be concentrated on conducting a real-world experiment of a reasonable scale authentication mechanism based on the created model. This will make possible to compare theoretical and experimental results to verify the model and tune its numerical parameters.

REFERENCES

[1] Wang, Z., Crowcroft, J., "Quality-of-service routing for supporting multimedia applications", IEEE JSAC, vol. 14, no. 7, pp. 1228-1233, 1996 DOI: 10.1109/49.536364

[2] "Qualinet White Paper on Definitions of Quality of Experience" Output from the fifth Qualinet meeting, Novi Sad, March 12, 2013 Version 1.2

[3] Reichl, P., Egger, S., Möller, S., Kilkki, K., Fiedler, M., Hossfeld, T., Tsiaras, Ch., Asrese, A., "Towards a comprehensive framework for QoE and user behavior modelling", Seventh International Workshop on Quality of Multimedia Experience (QoMEX), 2015 DOI: 10.1109/QoMEX.2015.7148138

[4] Hossfeld, T., Fiedler, M., Tran-Gia, P., "A Generic Quantitative Relationship between Quality of Experience and Quality of Service", IEEE Network Special Issue on Improving QoE for Network Service, March 2010 DOI:10.1109/MNET.2010.5430142.

[5] Ciszkowski, T., Mazurczyk, W., Kotulski, Z., Hossfeld, T., Fiedler, M., Collange, D., "Towards Quality of Experience-based Reputation Models for Future Web Service Provisioning", Telecommunication Systems, Vol.51, No.4, pp.283-295, (2012) DOI: 10.1007/s11235-011-9435-2.

[6] Gerstel, O., Sasaki, G., "Quality of Protection (QoP): a quantitative unifying paradigm to protection service grades", in: SPIE Proc. OptiComm 2001, vol. 4599, (2001a), pp. 12–23 DOI: 10.1117/12.436060.

[7] "Quality of Protection Security Measurements and Metrics", Editors: Gollmann, Dieter, Massacci, Fabio, Yautsiukhin, Artsiom (Eds.), Springer 2006 DOI: 10.1007/978-0-387-36584-8.

[8] Księżopolski, B., Kotulski, Z., "Adaptable security mechanism for dynamic environments", Computers & Security, Vol.26, No.3, pp.246-255, (2007) DOI: 10.1016/j.cose.2006.11.002.

[9] Siewruk G., Średniawa M., Grabowski S., Legierski J. , "Integration of context information from different sources: Unified Communication, Telco 2.0 and M2M", Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 851–858

[10] Schilit, B., Adams, N., Want, R., "Context-Aware Computing Applications", Proceeding WMCSA '94 Proceedings of the 1994 First Workshop on Mobile Computing Systems and Applications, pp.: 85 – 90 DOI: 10.1109/WMCSA.1994.16.

[11] Pascalau E., Nalepa G.J., Kluza K., "Towards a Better Understanding of Context-Aware Applications", Proceedings of the 2013 Federated Conference on Computer Science and Information Systems pp. 959–962

[12] Wrona, K., Gomez, L., "Context-aware security and secure context- awareness in ubiquitous computing environments", XXI Autumn Meeting of Polish Information Processing Society, Conference Proceedings, pp.: 255 – 265

[13] Alves, P., Ferreira, P., Radiator, "Efficient message propagation in context-aware systems", in Journal of Internet Services and Applications, 2014, DOI: 10.1186/1869-0238-5-4.

[14] Orynczak, G., Kotulski, Z., "Context-Aware Secure Routing Protocol for Real-Time Services", in: Cryptography and Security Systems, Volume 448 of the series Communications in Computer and Information Science pp 193-207, Springer 2014 DOI: 10.1007/978-3-662-44893-9_17.

[15] Wenning, B-L., "Context-Based Routing", in Dynamic Networks, Springer 2010 DOI: 10.1007/978-3-8348-9709-1.

[16] Goel, D., Kher, E., Joag, S., Mujumdar, V., Griss, M., Dey, A. K., "Context-Aware Authentication Framework", Proc. First Annual Conference on Mobile Computing, Applications, and Services (MobiCASE 2009), pp. 26-29 DOI: 10.1007/978-3-642-12607-9_3.

[17] Lenzini, G., "Trust-Based and Context-Aware Authentication in a Software Architecture for Context and Proximity-Aware Services", in Architecting Dependable Systems VI Volume 5835 of the series Lecture Notes in Computer Science, 2009, pp. 284-307 DOI: 10.1007/978-3-642-10248-6_12.

[18] Park, S., Han, Y., Chung, T., "Context-Aware Security Management System for Pervasive Computing Environment", in Modeling and Using Context Volume 4635 of the series Lecture Notes in Computer Science pp 384-396, August 2007, pp. 20-24 DOI: 10.1007/978-3-540-74255-5_29.

[19] Hayashi, E., Das, S., Amini, S., Hong, J., Oakley, I., "CASA: Context- Aware Scalable Authentication", Proc. of the Ninth Symposium on Usable Privacy and Security, ISBN 978-1-4503-2319-2, July 2013 DOI: 10.1145/2501604.2501607.

[20] Kulkarni, D., Tripathi, A., "Context-aware role-based access control in pervasive computing systems", Proc. of the 13th ACM symposium on Access control models and technologies (SACMAT '08), June 2008, pp. 113-122 DOI: 10.1145/1377836.1377854.

[21] Chun-Dong, W., Ting, L., Li-Chun, F., "Context-Aware Environment-Role-Based Access Control Model for Web Services", in Multimedia and Ubiquitous Engineering, ISBN 978-0-7695-3134-2, April 2008, pp. 288 – 293 DOI: 10.1109/MUE.2008.77.

[22] Khan, M., F., F., Sakamura, K., "Context-aware access control for clinical information systems" , in Innovations in Information Technology (IIT), ISBN 978-1-4673-1100-7, March 2012, pp. 123 – 128 DOI: 10.1109/INNOVATIONS.2012.6207715

[23] Krawczyk, H., Lubomski, P., "User Trust Levels and Their Impact on System Security and Usability", Proc. of

22nd International Conference Computer Networks, ISBN 978-3-319-19418-9, May 2015, pp. 82 – 91 DOI: 10.1007/978-3-319-19419-6_8

[24] Furnell, S., M., Jusoh, A., Katsabas, D., "The challenges of understanding and using security: A survey of end - user", in Computers and Security vol. 25 issue 1, February 2006, pp. 27 – 35 DOI: 10.1016/j.cose.2005.12.004.

[25] Furnell, S., "Usability versus complexity – Striking the balance in end – user security ", in Network Security, December 2010, pp. 13 – 17 DOI: 10.1016/S1353-4858(10)70147-1.

[26] Wu, D., Zhang, H., Wang, H., Wang, C., Wang, R., Xie, Y., "Quality of protection – driven data forwarding for intermittently connected wireless networks", in IEEE Wireless Communications vol. 22 issue 4, August 2015, pp. 66 – 73 DOI: 10.1109/MWC.2015.7224729.

[27] Li, H., Liu, D., Dai, Y., Luan, T., H., „Engineering searchable encryption of mobile cloud networks: when QoE meets QoP", in IEEE Wireless Communication vol. 22 issue 4, August 2015, pp. 74 – 80 DOI: 10.1109/MWC.2015.7224730.

[28] Wang, W., Zhang, Q., "Toward long-term quality of protection in mobile networks: a context-aware perspective", in IEEE Wireless Communications vol. 22 issue 4, August 2015, pp. 34 – 40 DOI: 10.1109/MWC.2015.7224725.

[29] Lorentzen, C.; Fiedler, M.; Johnson, H.; Shaikh, J.; Jrstad, I., "On user perception of web login — A study on QoE in the context of security", in Telecommunication Networks and Applications Conference (ATNAC), Auckland, Oct. 31 2010-Nov. 3 2010, pp. 84 – 89 DOI: 10.1109/ATNAC.2010.5680262

[30] Lorentzen, Ch., "User Perception and Performance of Authentication Procedures", Thesis, Blekinge Institute of Technology, School of Computing, 2011.

[31] Lorentzen, Ch., "On User Perception of Authentication in Networks", PhD. Thesis, Blekinge Institute of Technology 2014.

[32] Sepczuk, M., "Security oriented on user's perception in cloud computing", in Przegląd Telekomunikacyjny, no. 8-9, 2013, pp. 1245 – 1251.

[33] Crawford, H., Renaud, K., "Understanding user perceptions of transparent authentication on a mobile device", in Journal of Trust Management vol. 1 issue 1, June 2014 DOI: 10.1186/2196-064X-1-7.

[34] Eliasson; Ch., Fiedler, M.; Jørstad, I., "A Criteria-Based Evaluation Framework for Authentication Schemes in IMS", ARES '09. International Conference on Availability, Reliability and Security, 2009 DOI: 10.1109/ARES.2009.166.

[35] Kotulski, Z., Sepczuk, M., Sitek, A., Tunia, M. A., „Adaptable Context Management Framework for Secure Network Services", in Annales UMCS Informatica, vol. 14, no.2, September 2014, pp. 7 – 30 DOI: 10.2478/umcsinfo-2014-0013.

[36] Sepczuk, M., "Authentication Mechanism Based on Adaptable Context Management Framework for Secure Network Services", in Annales UMCS, Informatica, vol. 14, no.2, September 2014, pp. 31-44 DOI: 10.2478/umcsinfo-2014-0010.

[37] Irvine, C., Levin, T., "Quality of Security Service", Proceeding NSPW '00 Proceedings of the 2000 workshop on New security paradigms, Pages 91 - 99, doi: 10.1145/366173.366195.

[38] EL Yamany, H., F., Capretz, M., Allison, D., S., "Quality of Security Services for Web Services within SOA", in Congress on Services – I, July 2009, pp.: 653 – 660 DOI: 10.1109/SERVICES-I.2009.95.