Quantifying Usability and Security in Authentication

Martin Mihajlov
E-business Department, Faculty of Economics
Skopje, Macedonia
martin@eccf.ukim.edu.mk

Borka Jerman Blažič
Jožef Stefan Institute
Ljubljana, Slovenia
borka@e5.ijs.si

Saso Josimovski
E-business Department, Faculty of Economics
Skopje, Macedonia
sasojos@eccf.ukim.edu.mk

ABSTRACT
Substantial research has been conducted in developing sophisticated security methods with authentication mechanisms placed in the front line of defense. While the effectiveness of these systems is known, it is not always clear how they contribute to the overall usability and security of the system. To address this, we propose a quantification scheme to define a quality score for each criterion.

2. QUANTIFICATION APPROACH
When deciding on an evaluation method for a particular system or task, different quality criteria exist. Many security and usability aspects can be taken into consideration for evaluation; nonetheless, not all of them might be descriptively applicable. The quantification approach for evaluating usability and security in authentication mechanisms presented in this paper uses quality criteria stemming from an idea suggested by Renaud [3]. By properly adapting the criteria to authentication mechanisms and adding contextual flexibility, the focus on the presented approach is to concurrently evaluate both security and usability aspects of the system. As authentication mechanisms have shortcomings in both areas, two deficiency dimensions are identified, one for security and one for usability. In addition, each deficiency dimension consists of several quality criteria, defined through composite parameters, which are used to derive a value for the deficiency dimension as explained in the following section.

2.1. Quantifying Quality Criteria
Quantification refers to the binding of signs of quantity to a predicate or a subject of a proposition. Thus in the quantification process a particular aspect of an artifact is measured or expressed in terms of a quantity [4]. The quantification process proposed in this paper is the application of a set of metrics to specified quality criteria in order to determine a particular value. The proposed scheme, unlike most quality measurement schemes, does not use quality metrics, but focuses on the quality of the system in terms of its suitability for the task in a particular domain. To formulate the quantitative specifications a proposal by Gilb [5] is followed which consists of the following steps: identify the quality criteria, assign scales of measure to quality criteria, and identify the required quality levels. Following these guidelines, the next section presents a quantification scheme, defines the quality criteria and assigns the integrated scales of measures.

2.2. Defining Quality Criteria and Measurements
As we have established the two quality dimensions of the quantification scheme: usability and security, the next step is to determine the composite parameters that will be used to calculate the quality value. With respect to each quality criteria of the dimension its deficiency will be determined in order to define the quality of the system by deriving the
quality coefficient for a particular authentication mechanism. Each quality criteria is assigned a value ranging from 0 to 1, where 0 signifies a high quality deficiency, while 1 signifies no quality deficiency. These values are then used to indicate the deficiency of a particular authentication mechanism for each dimension. Once all deficiency values have been determined, the final generic quality coefficient can be calculated. The mechanism outlined below proposes one possible way of quantifying the quality of authentication mechanisms to support measured comparison.

In the assignment of values in the 0 to 1 range the quantification scheme has defined scoring intervals. Depending on the nature of the quality coefficient the scoring intervals can be defined through the following two approaches.

**Participation.** If the quality coefficient is influenced by $n$ parameters each parameter participates in the total quality coefficient with a $1/n$ score. All of the parameters have an equal weight, unless there are clear indications that there is a different weight distribution.

**Categorization.** If the quality coefficient is influenced by 1 parameter then $n$ specific level categories are defined with the level intervals belonging in $[0, 1/n)$, $[1/n, 2/n)$, $[(n-1)/n, 1]$ ranges.

The purpose of this quantification proposal is to help the evaluator determine the interval for the quality coefficient value. The exact participative or level value is determined by the expert evaluator.

### 3. SECURITY EVALUATION

Although related and interdependent, the quality criteria of the security dimension exhibit disparate characteristics; therefore, they are treated as separate entities. Based on an authentication overview [6] the quantification scheme includes the following 5 security characteristics: secrecy, abundance, revelation, privacy and breakability.

#### 3.1. Secrecy

The predictability of an authentication key is a big issue as confirmed by the plethora of password choice recommendations in professional and popular literature [7]. The difficulty of intentional unpredictability arises with the poor concept of randomness that human beings posses. To determine if a sequence is random it is necessary to observe several properties: even distribution, the equal probability of distribution over the entire set of data, distinctness, the nonexistence of relationship with previous or subsequent data, and uniqueness, the inability to randomly produce the same sequence of data. The score for the secrecy criteria is assigned based on how many people find the key predictable, with the highest score going to completely unpredictable authentication. Each of the properties defined above: even distribution, distinctness and uniqueness are graded in a low/average/high category and have a 1/3 participation towards the total scoring for this criterion. The scoring details are presented in Table 1.

<table>
<thead>
<tr>
<th>Even distribution</th>
<th>Low</th>
<th>Average</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0-0.11</td>
<td>0.11-0.22</td>
<td>0.22-0.33</td>
</tr>
<tr>
<td>Distinctness</td>
<td>0-0.11</td>
<td>0.11-0.22</td>
<td>0.22-0.33</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>0-0.11</td>
<td>0.11-0.22</td>
<td>0.22-0.33</td>
</tr>
</tbody>
</table>

Table 1. Quantifying Secrecy based on random properties.

#### 3.2. Abundance

Abundance measures the authentication key password space in two aspects: the number of available keys counterbalanced by the number of keys commonly used in practice. This has a direct effect on the breakability of the authentication key with more possibilities increasing the time required to compromise the key.

Based on the available set, key length and repetition the password space ($P_s$) can be usually calculated with either a combination or a permutation formula [8]:

$$P_s = \frac{(n + r - 1)!}{r!((n-1)!)} \quad \text{or} \quad P_s = n^r$$

To quantify the abundance criteria we conditionally categorize the value ranges based on the password space (see Table 2).

<table>
<thead>
<tr>
<th>Value</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 – 0.33</td>
<td>If $P_s &lt; 10^6$</td>
</tr>
<tr>
<td>0.33 – 0.66</td>
<td>If $10^6 &lt; P_s &lt; 10^{12}$</td>
</tr>
<tr>
<td>0.66 – 1</td>
<td>If $P_s &gt; 10^{12}$</td>
</tr>
</tbody>
</table>

Table 2. Quantifying Abundance based on password space.

#### 3.3. Revelation

Revelation measures the disclosure level of the authentication key from a user and system perspective. To quantify this quality criterion both points of authentication key revelation have to be considered. As they are divided into system revelation and user revelation, each type can act as a deficiency parameter and decrease the score up to 0.5.

#### 3.4. Privacy

Privacy measures the amount of private details required by the authentication mechanism. The compromised key violates the person's privacy and could result in identity theft [9]. Depending on the level of private data available when the system is compromised, and the level of risk factor for identity theft, different deficiency scoring will be calculated based on participation. The default quantification value is 1, with each personal data required by the system affecting this value with a negative score of 0.25. The details are presented in Table 3.
### Table 3. Quantifying Privacy based on personal data.

<table>
<thead>
<tr>
<th>Value</th>
<th>Private data</th>
</tr>
</thead>
<tbody>
<tr>
<td>-0.25</td>
<td>Full name</td>
</tr>
<tr>
<td>-0.25</td>
<td>Date of birth</td>
</tr>
<tr>
<td>-0.25</td>
<td>Email</td>
</tr>
<tr>
<td>-0 to 0.25</td>
<td>Additional data</td>
</tr>
</tbody>
</table>

#### 3.5. Breakability

Breakability refers to the effort necessary to work around the security mechanism to gain access to either the system or the algorithm that generates the authentication key. Depending on the system the attacker can use one of four different categories of attack techniques to discover the key: research, brute-force, dictionary and keylogging. To quantify the breakability quality criteria, the susceptibility to every attack category needs to be evaluated. Participatively, every categorical vulnerability creates a 0.25 deficiency.

### 4. USABILITY EVALUATION

Authentication mechanisms require cognitive activity on some level; therefore it is important to consider the user information-processing characteristics which directly determine the success of the authentication mechanism. The proposed quantification scheme includes 5 usability criteria: meaningful retrieval, processing depth, requirements, convenience and inclusivity.

#### 4.1. Processing depth

In essence, the processing depth quality criteria measures the cognitive activity involved in the authentication encoding process. The depth of processing at encoding time is determined by the amount of attention paid to the activity [10]. The activity involved in the encoding of an authentication key will determine how well the user can retrieve the key later. The quantification of this criterion will be based on assigning values for particular categories of activity. Depending on the activity category the assigned value will range between the given values for the cognitive, visual and rehearsal categories as presented in Table 4.

<table>
<thead>
<tr>
<th>Category</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>No effort</td>
<td>1</td>
</tr>
<tr>
<td>Cognitive</td>
<td>0.67-0.99</td>
</tr>
<tr>
<td>Visual</td>
<td>0.34-0.66</td>
</tr>
<tr>
<td>Rehearsal</td>
<td>0.0-0.33</td>
</tr>
</tbody>
</table>

#### 4.2. Meaningful retrieval

Meaningful retrieval is measured by the mental effort the user has to use to retrieve and deduce the authentication key. A previously-recorded item will be forgotten due to one of the following reasons: decay, this can happen if the item was not encoded specifically enough and the person cannot retrieve it, interference, this happens when an item in memory interferes with another item, and recall failure, a diminishing number of established connections with previous structures in long-term memory.

Table 5 presents a suggestive scheme for quantifying Meaningful retrieval based on type of effort and retrieval method. The values are assigned as such considering that users typically deal with authentication as a necessary evil. Consequently, a no effort system will have the least deficiency as this goes along with the principle of psychological acceptability. Recognition and recall are highly dependable on the authentication key, thus scored differently depending on the meaningfulness of the key.

<table>
<thead>
<tr>
<th></th>
<th>Deducible</th>
<th>Cued</th>
<th>Uncued</th>
<th>System assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>No effort</td>
<td>1.00-0.88</td>
<td>1.00-0.76</td>
<td>1.00-0.63</td>
<td>1.00-0.51</td>
</tr>
<tr>
<td>Recognition</td>
<td>0.88-0.76</td>
<td>0.75-0.63</td>
<td>0.62-0.51</td>
<td>0.50-0.01</td>
</tr>
<tr>
<td>Recall</td>
<td>0.75-0.51</td>
<td>0.50-0.26</td>
<td>0.25-0.01</td>
<td>0.00</td>
</tr>
</tbody>
</table>

#### 4.3. Requirements

Requirements measure the resources required for software, hardware and technical support of the authentication mechanism. To quantify requirements, the minimum hardware and/or software system configuration needs to be addressed as well as the technical expertise necessary to support the authentication mechanism. Thus, the existence of each requirement would influence the deficiency of the system by up to a third of its value. The value of 1 is assigned when no additional resources are required, 0.67 is assigned when, for example, special software is needed, 0.33 would be assigned if both special software and hardware are required and 0 is assigned when technical support is included in the set along with software and hardware.

#### 4.4. Convenience

User’s compliance to security requests is very limited as they are sensitive to systems that waste their time [11]. Convenience measures the time spent at enrollment, authentication and replacement. In the quantification methodology, as authentication time is most important, it can affect the deficiency of the convenience quality criteria for a value of up to 0.7 for time-consuming authentication. A participation of 0.1 is assigned if the mechanism is time-consuming at enrolment and a 0.2 is if the mechanism is time-consuming at replacement.
4.5. Inclusivity

Inclusivity ensures that everyone, regardless of cognitive, mobility and sensory skills, can use the authentication mechanism [12]. This includes disabilities such as hearing, sight, mobility, learning and color, which are relevant in an authentication context. In the quantification scheme this criteria is quantified by calculating the inclusion of users in disability categories. A lower score is assigned when a particular group is barred from access, with a growing score deficit as more categories are excluded. This can be easily defined on a scale from 0 to 1, as the percentage of excluded users is subtracted. For example, a text-based authentication mechanism will have an inclusivity value of 0.85 as 15% of the population is excluded due to dyslexia, thus having problems with remembering words.

5. CONCLUSION

Theoretical secure authentication is possible; however, despite the influence of usability, little research has been focused on the balance between usability and security to optimize secure use of the ICT systems. As current usability evaluation methods are focused only on usability and are not considerate of system security they offer insufficient methodologies to evaluate usable security. In this paper this issue was engaged by proposing a quantification approach for assessing usable security in authentication mechanisms. The scheme defined usability and security quality criteria which where individually quantified through a quality coefficient. The quantification scheme of the quality criteria assumed linear dependence between different quality criteria parameters. For simplification it also considered the different quality criteria as mutually independent variables.

The foundation of the quantification scheme can be expanded to an evaluation framework which can guide the evaluation process of any security system, not just authentication mechanisms. Initially, the precise usability and security criteria for the system have to be determined, evaluated and then quantified to determine the total quality of the system. This evaluation framework for usable security has many additional aspects that can be explored and developed further. As both security and usability quality criteria can exhibit nonlinear properties, a more active measurement can be provided upon additional research. In addition, some quality criteria are interdependent which would require a different quantification approach as their performance and scoring is not autonomous. The dependencies between specific criteria need to be researched in order to improve the quantification approach for each value. Furthermore, a more precise mathematical definition of each function will have to be based on experimental data which is a subject of future study. Based on these explorations the framework will be greatly improved which is a necessary step in developing an organized research program toward addressing usability issues in authentication security.

REFERENCES