Supporting Decision Makers in Choosing Suitable Authentication Schemes

P. Mayer[1], S. Neumann[1], D. Storck[1] and M. Volkamer[1,2]

[1]SECUSO - Security, Usability, and Society - Technische Universität Darmstadt
[2]Privacy and Security Research Group - Karlstad University
e-mail: {firstname.lastname}@secuso.org

Abstract

Despite its well-known deficiencies, the text password remains ubiquitous. Researchers previously suggested that this apparent conundrum was due to the complexity of choosing a suitable authentication scheme with respect to the desired application scenario. The plethora of alternatives can leave decision makers flummoxed and leads to their reaching for the familiar text password. To alleviate these difficulties, Renaud *et al.* suggested ACCESS (Authentication ChoiCE Support System), an abstract framework to support decision makers in this struggle. In this paper we present the first concrete realization of ACCESS. We create a knowledge base from the results of a literature review and present a technique which allows decision makers to specify their requirements effortlessly. The central contribution of this work is the realization of ACCESS' feasibility analysis based on an adapted Analytic Hierarchy Process (AHP). This adaptation allows outsourcing the burden of knowing all authentication alternatives to experts, while keeping the complexity of the expert part as low as possible.

Keywords

Authentication, Decision Support, Analytic Hierarchy Process

1. Introduction

Despite a unanimous desire by researchers, users, and decision makers alike to replace the text password, it remains the prevalent authentication scheme (Herley & van Oorschot 2012; Renaud et al. 2014). One of the primary reasons, as identified by Renaud *et al.* (2014), is that decision makers feel overwhelmed when confronted with the plethora of available alternatives. To address this issue, Renaud *et al.* proposed the framework ACCESS (Authentication ChoiCE Support System). It defines the following abstract process to support decision makers in identifying the most suitable authentication scheme(s) for their application scenario: First, ACCESS requires the decision maker to enter the requirements of her/his application scenario in terms of features a suitable authentication scheme must provide (e.g. accessibility aspects or resistance against relevant attacks). Then, a feasibility analysis is executed to identify the most suitable authentication schemes with respect to the specified requirements among all the schemes in ACCESS' knowledge base. The result of this process is a number of ranked alternatives for consideration. However, ACCESS does not specify how this process should be implemented in practice. Figure 1 depicts ACCESS' abstract process with all elements involved.

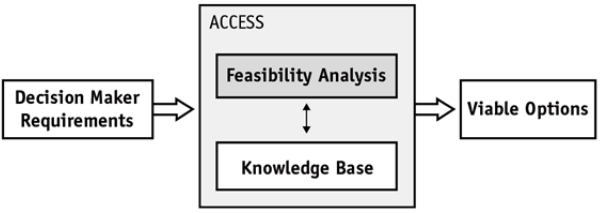

Figure 1: The ACCESS decision support framework

The goal of this paper is to provide the first concrete realization of ACCESS' abstract process. We build the knowledge base from the results of a literature review (section 2). Then we define how decision makers should specify their requirements (section 3). Thereafter, we present the main contribution of this paper: the implementation of the feasibility analysis using the Analytic Hierarchy Process (AHP) (Saaty 1988), an established approach for decision problems (section 4).

2. Knowledge Base

Our first step in the realization of ACCESS was a literature review to identify relevant authentication schemes and their features. The results of this literature review serve as foundation for ACCESS' *knowledge base*. Due to space constraints we forgo the details, which can be found the accompanying technical report (Mayer et al. 2016).

2.1. Authentication Schemes

Bonneau *et al.* (2012) present an extensive review in which they identify a list of 36 authentication schemes. We extended this list with recent developments which we believe to be valuable additions, namely: FilmPW (Catuogno & Galdi 2013), CaRP (Zhu et al. 2014), Xside (De Luca et al. 2014), Face (Findling & Mayrhofer 2012), Palm Veins (Watanabe 2008), Facebook social auth (Hicks 2011), and KinWrite (Tian et al. 2013). Furthermore, we added older schemes not considered by Bonneau *et al.*, since recent papers present user studies providing more reliable data than previously available. The schemes we added are: PassPoints (Wiedenbeck et al. 2005), CCP (Chiasson et al. 2007), and Passfaces (Passfaces Corporation 2006). Lastly, we also excluded one authentication scheme (the Hopper and Blum scheme), since, in the meantime, it has been deemed unsuitable for actual usage (Asghar 2012). Thus, the overall number of schemes included in our knowledge base is 45.

2.2. Authentication Scheme Features

ACCESS (Renaud et al. 2014) defines multiple authentication scheme features over five dimensions. However, these features remain abstract and difficult to measure (e.g. the convenience feature includes multiple metrics). Therefore, we adopt the 25 features used by Bonneau *et al.* (2012) in their survey. To increase the granularity, we define further sub-features for each feature based on the quasi-assignments of

Bonneau *et al.* (e.g. the memorywise-effortless feature is split into the sub-features *no secret to remember*, *one secret to remember*, and *more than one secret to remember*). Due to space constraints, detailed definitions of the features and their sub-features are beyond the scope of this paper, but are available in the technical report (Mayer et al. 2016). Note, that we also distinguish between additive and selective features. For selective features, only one sub-feature can be assigned to an authentication scheme at any time (e.g. the memorywise-effortless feature explained above belongs to this category). For additive features, an authentication scheme can be assigned multiple sub-features (e.g. when considering the feature infrequent-errors, a scheme can be *not susceptible to input errors* as well as *not susceptible to assignment errors*).

3. Specification of the Decision Maker Requirements

Despite being well aware of the text password's problems, decision makers continue to reach for this familiar option (Renaud et al. 2014). Renaud *et al.* identify as reason for this apparent conundrum the complexity of weighing all viable authentication schemes: decision makers simply feel overwhelmed.

Therefore, we aim to render the specification of the requirements for the decision makers as effortless as possible. Our implementation lets decision makers (1) specify hard constraints (i.e. mandatorily required features), and (2) partially rank features to specify the relative importance of features (allowing tied values in case multiple features are equally important). Figure depicts a prototype interface for the specification of decision maker requirements. Each feature can be individually selected and dragged to have the desired rank among all features. The further to the top a feature is placed, the higher is its importance. Also, as can be seen in Figure 2 for the top-most feature (resilient-to-physical-observation), single sub-features can be selected as hard constraints making them mandatorily required by suitable schemes.

Figure 2: Requirement specification in the ACCESS user interface

4. Feasibility Analysis

Based on the decision maker requirements, the feasibility analysis identifies the most suitable authentication schemes among all those available in the knowledge base. It supports multiple decision criteria (in ACCESS given by the decision maker requirements specified along the authentication scheme features) and a finite number of potential solutions (in ACCESS given by the authentication schemes). As such, the feasibility analysis represents an instantiation of the multiple criteria evaluation problem. The analytic hierarchy process (AHP) (Saaty 1988) is an established approach to solving such problems. It is particularly adequate for our realization because it can be easily adapted to work reliably even in the face of an incomplete specification of the application scenario by the decision maker.

The implementation of the feasibility analysis using the AHP represents the main contribution of this paper. In the following we will first describe the general AHP methodology and present the challenges that arise from employing it for the feasibility analysis. Secondly, we present the adapted AHP we use to address these challenges. Thirdly, we describe the implementation of the adapted AHP.

4.1. The Analytic Hierarchy Process (AHP)

In this subsection we describe the general working principles of the AHP and point out challenges which arise from utilizing it to realize ACCESS' feasibility analysis.

4.1.1. Summary of the AHP

AHP provides a means to determine attribute scores on the basis of small and manageable pairwise comparisons. According to its inventor Saaty (2008), AHP comprises four sequential steps which are depicted in Figure 3.

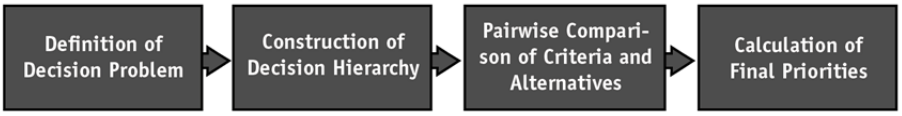

Figure 3: The Analytic Hierarchy Process (Saaty 2008)

A decision problem starts with the collection of information relevant to the decision, i.e. the goal of the decision, criteria that influence the quality of a solution to the problem, and alternatives as potential solutions to the problem (*definition of the decision problem*). After its definition, the decision problem is structured in a hierarchical manner (*construction of decision hierarchy*). The root node of the hierarchy represents the goal of the decision problem. On the second level of the hierarchy, criteria contributing to the goal are expressed. On the level of criteria, one or more hierarchy levels can be defined. On the lowest level of the hierarchy, decision alternatives are compared in a pairwise manner with regard to the criterion under consideration. To build the basis for a decision, for any element on one

specific hierarchy level (excluding the leaf level) a pairwise comparison of all child-elements is conducted (*pairwise comparison of criteria and alternatives*). AHP provides a numerical scale $[\frac{1}{9}, 9]$ to rate pairwise comparisons. The results of these pairwise comparisons are stored in a local comparison matrix S. If two alternatives A_k and A_l perform equally well, then the matrix entries s_{kl} and s_{lk} are assigned both the value 1. If A_k performs extremely better than A_l, then s_{kl} is assigned the value 9, while s_{lk} is assigned the value $\frac{1}{9}$. Intermediate values on the numerical scale are 3, 5, and 7 and their reciprocal values respectively. This matrix forms the basis for priority vectors (refer to (Saaty 1988) for the details of the computation). Note that the pairwise comparisons of elements might lead to a violation of transitivity. AHP measures this violation of transitivity in terms of a consistency ratio (CR). The literature (Karlsson & Ryan 1997; Ishizaka & Labib 2009) widely agrees that CR values below 10% are acceptable. Ultimately, global priorities for decision alternatives are calculated (*calculation of final priorities*). Therefore, priorities of one hierarchy level constitute weights of the next lower hierarchy level. On the lowest level of the hierarchy, the *m* alternatives are globally prioritized with regard to *k* criteria. The final priority values of the alternatives are consequently the sum of all weighted priority values for the alternatives with regard to the lowest level criteria.

4.1.2. Challenges of using the AHP for the Feasibility Analysis

Need for Expert Knowledge. In its conventional form, the AHP serves decision makers to structure their knowledge regarding decisions to be taken, i.e. they specify the relative importance of decision criteria to the overall decision goal as well as the relative performance of alternatives to decision criteria. In the context of authentication schemes, it is exactly the lack of knowledge that prevents decision makers from abandoning established schemes and moving towards more adequate schemes. The first challenge is therefore to augment AHP by authentication expert knowledge.

Transformation of Decision Maker Requirements into AHP Weights. Our realization of ACCESS accommodates for the possibly incomplete knowledge of decision makers with respect to their application scenario by offering an interface to specify requirements by setting hard constraints and partially ranking the available features. The second challenge is therefore to translate this input of the decision maker into weights for each feature as needed by the AHP.

Scale Values. To conduct and quantify pairwise comparisons between authentication schemes with regard to several features, measurable differences of the authentication schemes have to be assigned to AHP scale values. The third challenge is therefore to map pairwise authentication scheme comparisons to AHP scale values.

Complexity of the Analytic Hierarchy Process. The pairwise comparisons of decision criteria and decision alternatives with respect to decision criteria make the practicability of the decision process sensitive to the number of decision criteria and

decision alternatives. The fourth challenge is therefore to reduce the complexity of the decision process.

4.2. Adapting AHP for Use in our Feasibility Analysis

In this subsection we address the challenges pointed out above. The basic structure of the feasibility analysis is shown in Figure 4 and is explained throughout this section.

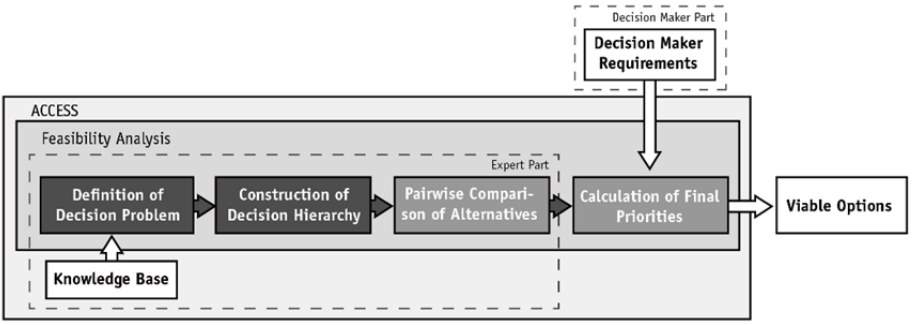

Figure 4: Realization of ACCESS' feasibility analysis by means of the adapted Analytic Hierarchy Process

4.2.1. Need for Expert Knowledge

To compensate for the lack of decision maker knowledge, we divide the AHP into two parts: one part that is to be executed by the decision makers (depending on their application environment using the technique explained in section 3) and one part that is to be executed by authentication experts (as explained in the following). As the pairwise comparison of authentication schemes with regard to features is not influenced by decision makers' requirements, the comparisons are conducted by authentication experts. Furthermore, the definition of the decision problem as well as the construction of the decision hierarchy are static for all authentication scheme decision problems. Consequently, the decision makers provide their requirements only prior to the calculation of final priorities, namely the last AHP step (see Figure).

4.2.2. Transformation of Decision Maker Requirements into AHP Weights

The specification of hard constraints serves to exclude authentication schemes from further consideration. Once inappropriate schemes have been excluded, the remaining schemes are prioritized according to the (partial) feature ranking, thereby facilitating the decision makers' *a posteriori* decision process. The positions of selected features in the feature list $F = (f_1, \dots, f_n)$ dissemble the feature list into ranges of equally important features and specifically prioritized features.

Each selected feature is assigned the inverse value of its specified position. Non-selected features between two selected features f_k and f_l are treated as equally

important. They obtain uniformly the inverse of the arithmetic mean between the selected features. Formally, this is expressed as follows:

$$\tilde{w}_i = \begin{cases} |F| - i & \text{if} f_i \text{ selected} \\ |F| - (\sum_{j=k+1}^{l-1} j)/(k-l-1) & \text{otherwise} \end{cases}$$

The weight values are normalized to obtain the final priority vector W_F:

$$w_i = \tilde{w}_i / (\sum_{j=1}^{n} \tilde{w}_j) \qquad W_F = [w_1, \ldots, w_n]^T$$

4.2.3. Scale values

To conduct the pairwise comparisons of authentication schemes with regard to features, we make explicit use of the sub-features (as explained in section 2.2). In the case of selective sub-features, the maximum difference between two alternative sub-features is mapped to the scales values $\left(9, \frac{1}{9}\right)$, while smaller differences can be mapped linearly. In the case of additive sub-features, the difference between the satisfaction of all sub-features and the satisfaction of no sub-feature can be mapped to scales values $\left(9, \frac{1}{9}\right)$, while again smaller differences can be mapped linearly. Consider for instance the selective feature *memorywise-effortless* already mentioned in section 2.2. The feature comprises the three sub-features *no secret to remember*, *one secret to remember* and *more than one secret to remember*. In case two schemes with equally many secrets to remember are compared, the scale values $(1,1)$ are assigned. In case a scheme with *no secret to remember* is compared to a scheme with *more than one secret to remember*, the scale values $\left(9, \frac{1}{9}\right)$ are assigned. For the remaining difference (*no secret to remember* vs *one secret to remember* and *one secret to remember* vs. *more than one secret to remember)*, we assign the intermediate value between 1 and 9, namely 5 and the respective reciprocal value $\frac{1}{5}$, resulting in the scale values $(5, \frac{1}{5})$.

4.2.4. Complexity of the Analytic Hierarchy Process

Using the technique explained in section 3 allows us to hide the complexity of the AHP from the decision maker. The same is not true for the expert part of our adapted AHP. Given the set of 25 features and 45 authentication schemes, the number of $25 \cdot \frac{45 \cdot (44-1)}{2}$ comparisons becomes a practical limitation for the expert part of the feasibility analysis process. In order to reduce this complexity, *equivalence classes of authentication schemes* are constructed on the basis of sub-features (e.g. for the feature memorywise-effortless, there exist three equivalence classes: the schemes with *no secret to remember*, the schemes with *one secret to remember*, and the schemes with *more than one secret to remember*). Given n sub-features, selective features result in n equivalence classes and additive sub-features result in 2^n

equivalence classes. Rather than all authentication schemes, only the equivalence classes are compared against each other and mapped according to the adapted AHP scale (see second adaptation in section 4.2.3). To take subtle variations within equivalence classes into account, the interval scale is extended by two intermediate scale values, namely 1.5 and $\frac{2}{3}$. For example, two different authentication schemes might both belong to the class *one secret to remember*, but for one of the schemes the user's secret is her/his mother's maiden name, while for the other it is a complex 20-character text password chosen at random by the system. These two systems cannot be distinguished based on equivalence classes, but using the intermediate scale values it is nevertheless possible to acknowledge the difference between them.

4.3. Implementing the Expert Part of the Adapted AHP

It has been shown how the decision making process can be facilitated by the incorporation of expert knowledge into the AHP. This section is dedicated to the realization of the AHP's expert part, namely the definition of the decision problem, the construction of a decision hierarchy and the pairwise comparison of authentication schemes with regard to features.

4.3.1. Definition of Decision Problem

ACCESS supports decision makers in choosing the most suitable authentication schemes for their specific application scenario. This goal can be directly assigned to the AHP's problem statement. In Section 2.2, 25 features of authentication schemes have been identified as decision criteria for the determination of the most suitable authentication scheme(s). Furthermore, our literature review resulted in 45 authentication schemes constituting the set of possible solutions to the decision problem.

4.3.2. Construction of Decision Hierarchy

Under the core decision problem (i.e. the root node) two further hierarchy levels are specified. The first level of the decision hierarchy comprises the decision criteria, namely the 25 authentication scheme features. The second level comprises the decision alternatives, namely the 45 authentication schemes.

4.3.3. Pairwise Comparison of Alternatives

The adaptation of the AHP to the ACCESS framework requires two steps: First the construction of authentication scheme equivalence classes with regard to all features. Second, equivalence classes and schemes within equivalence classes are compared in a pairwise manner and mapped onto the adapted AHP scale. Due to space limitations, we describe these steps for one single feature, namely *memorywise-effortless*. The details for all features can be found in the technical report accompanying this publication (Mayer et al. 2016). The ordered sub-features are *no secret to remember* (highest priority), *one secret to remember*, and *more than one secret to remember* (lowest priority). The set of authentication schemes that provide

the same sub-feature constitute one equivalence class (see the example in section 4.2.4). The maximum difference between sub-features is given by the sub-features *no secret to remember* and *more than one secret to remember*. Consequently, the comparison of equivalence classes representing these sub-features results in scale values $(9, \frac{1}{9})$. The intermediate relation between the sub-features *no secret to remember* and *one secret to remember*, and *one secret to remember* and *more than one secret to remember* is assigned to scale values $(5, \frac{1}{5})$. Eventually, the resulting performance matrix is given in Table 1.

Memorywise-effortless	No secret to remember	One secret to remember	More than one secret to remember
No secret to remember	1	5	9
One secret to remember	1/5	1	5
More than one secret to remember	1/9	1/5	1

Table 1: Scale values for the feature memorywise-effortless derived from its three sub-features

5. Discussion and Conclusion

In this paper we present our realization of ACCESS, a decision support system for authentication schemes. The knowledge base used by the feasibility analysis is built using the authentication schemes and features identified by Bonneau *et al.* (2012) with additions from our own literature review. Our realization allows non-expert decision makers a (partial) specification of their requirements by ranking the authentication scheme features and selecting hard constraints using the sub-features. The central contribution of this work is the construction of the feasibility analysis based on an adapted Analytic Hierarchy Process (AHP). This allows us to outsource the burden of knowing all authentication alternatives to experts, while keeping the complexity of the expert part as low as possible through the introduction of equivalence classes of authentication schemes. Thus, the expert part can be reused for multiple feasibility analyses. It must be executed only once in the beginning or when new relevant research findings become available. This makes the expert part highly effective in practice. Our vision going forward is to extend our prototype implementation and make it available as a collaborative platform, where authentication experts can add their knowledge, challenge our assessments of the reviewed literature, and add further schemes. As Bonneau *et al.* (2012) already put it: 'to make progress, the community must better systematize the knowledge that we have regarding both passwords and their alternatives'. Our hope is to contribute to this effort by supplying this platform.

6. Acknowledgements

The research reported in this paper has been supported by the German Federal Ministry of Education and Research (BMBF) and by the Hessian Ministry of Science and the Arts within CRISP (www.www.crisp-da.de/). Furthermore, this work has

been developed within the project KMU AWARE which is funded by the German Federal Ministry for Economic Affairs and Energy under grant no. BMWi-VIA5-090168623-01-1/2015. The authors assume responsibility for the content.

7. References

Asghar, H.J., 2012. *Design and Analysis of Human Identification Protocols*. Macquarie University.

Bonneau, J., Herley, C., van Oorschot, P.C. & Stajano, F., 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In 2012 IEEE Symposium on Security and Privacy. IEEE, pp. 553–567.

Catuogno, L. & Galdi, C., 2013. Towards the design of a film-based graphical password scheme. In The 8th International Conference for Internet Technology and Secured Transactions. IEEE, pp. 388–393.

Chiasson, S., van Oorschot, P.C. & Biddle, R., 2007. Graphical password authentication using cued click points. In European Symposium on Research in Computer Security. Dresden: Springer, pp. 359–374.

De Luca, A., Harbach, M., von Zezschwitz, E., Maurer, M., Slawik, B.E., Hussmann, H. & Smith, M., 2014. Now you see me, now you don't - protecting smartphone authentication from shoulder surfers. In 32nd Annual ACM Conference on Human Factors in Computing. New York, USA: ACM, pp. 2937–2946.

Findling, R.D. & Mayrhofer, R., 2012. Towards face unlock: on the difficulty of reliably detecting faces on mobile phones. In 10th International Conference on Advances in Mobile Computing & Multimedia. New York, USA: ACM, pp. 275–280.

Herley, C. & van Oorschot, P., 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy*, 10(1), pp.28–36.

Hicks, M., 2011. A Continued Commitment to Security. *facebook.com*. Available at: https://www.facebook.com/notes/facebook/a-continued-commitment-to-security/486790652130 [Accessed October 2015].

Ishizaka, A. & Labib, A., 2009. Analytic Hierarchy Process and Expert Choice: Benefits and limitations. *OR Insight*, 22(4), pp.201–220.

Karlsson, J. & Ryan, K., 1997. A cost-value approach for prioritizing requirements. *IEEE Software*, 14(5), pp.67–74.

Mayer, P., Neumann, S., Storck, D., & Volkamer, M., 2016. Supporting Decision Makers in Choosing Suitable Authentication Schemes. Technical Report, Technische Universität Darmstadt. Available at: https://secuso.org/TUD-CS-2016-0121

Passfaces Corporation, 2006. *The Science Behind Passfaces*, Passfaces Corporation.

Renaud, K., Volkamer, M. & Maguire, J., 2014. ACCESS: Describing and Contrasting. In Human Aspects of Information Security, Privacy, and Trust. Springer International Publishing, pp. 183–194.

Saaty, T.L., 2008. Decision making with the analytic hierarchy process. *International Journal of Services Sciences*, 1(1), pp.83–98.

Saaty, T.L., 1988. What is the Analytic Hierarchy Process? In *Mathematical Models for Decision Support*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 109–121.

Tian, J., Qu, C., Xu, W. & Wang, S., 2013. KinWrite: Handwriting-Based Authentication Using Kinect. In Network and Distributed System Security Symposium.

Watanabe, M., 2008. Palm Vein Authentication. In *Advances in Biometrics*. London: Springer London, pp. 75–88.

Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A. & Memon, N., 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1-2), pp.102–127.

Zhu, B.B. et al., 2014. Captcha as Graphical Passwords - A New Security Primitive Based on Hard AI Problems. *IEEE Transactions on Information Forensics and Security*, 9(6), pp.891–904.