POSTER: Towards Collaboratively Supporting Decision Makers in Choosing Suitable Authentication Schemes

Peter Mayer* Stephan Neumann* Melanie Volkamer*†
*SECUSO - Security, Usability and Society, Technische Universität Darmstadt
†Privacy and Security Research Group, Karlstad University
{firstname.lastname}@secuso.org

ABSTRACT

In spite of the the issues associated with them, text passwords are the predominant means of user authentication today. To foster the adoption of alternative authentication schemes, Renaud et al. [4] proposed the ACCESS (Authentication ChoiCE Support System) framework. In prior work, we presented the first implementation of this abstract framework as a decision support system. In this work, we report on the current progress of expanding our prototype implementation into a collaborative authentication research platform. In addition to a decision support system, this platform also includes an interface to systematically access all the information in the knowledge base and collaborative features to facilitate the process of keeping the data for the decision support system current.

Keywords

Authentication, Decision Support, Collaboration, AHP

1. INTRODUCTION

Despite a unanimous desire by researchers, users, and decision makers alike to replace the text password, it remains prevalent [2, 4]. According to Renaud et al. [4] one of the reasons for this conundrum is that decision makers feel overwhelmed when confronted with the plethora of available alternatives. As a consequence, alternatives to text passwords have no chance of being integrated into software or services. To address this issue, Renaud et al. [4] proposed the ACCESS (Authentication ChoiCE Support System) framework. In previous work, we presented the first concrete implementation of ACCESS [3]. Thereby, we built a knowledge base from the results of a literature review, introduced a technique for decision makers to specify their requirements effortlessly, and describe the realization of ACCESS's feasibility analysis using an adapted Analytic Hierarchy Process (AHP). Figure 1 depicts this realisation with all its components.

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2989045

In this work, we present our progress regarding the vision adumbrated in [3]: the development of our prototype implementation into a collaborative authentication research platform, where authentication experts can add their knowledge, challenge our assessments of the reviewed literature, and add further schemes. The goal of our work is thereby to provide three modules for our platform: (a) an integrated decision support system based on our prior work, (b) systematic access to the information in the knowledge base, and (c) enhance the available data through the introduction of collaboration features. In the remainder of this paper, we describe the current state of each of these three modules.

2. DECISION SUPPORT SYSTEM

The first part of our collaborative authentication research platform is the decision support module. It is based on prior work [3] using three components: (1) a knowledge base of authentication schemes and authentication scheme features, (2) an interface for decision makers to specify their requirements, and (3) a feasibility analysis using an adapted Analytic Hierarchy Process (AHP) [5]. In the following we will shortly describe each of these components.

2.1 Knowledge Base

The knowledge base is built on the results of a literature review identifying relevant authentication schemes and their features.

Bonneau et al. [1] present an extensive review in which they identify a list of 36 authentication schemes. We extended this list with recent proposals which are valuable additions and older schemes for which recent user studies provide more reliable data than previously available (the details can be found in [3]). The overall number of schemes included in our knowledge base is 45.

The authentication scheme features defined by ACCESS remain abstract and difficult to measure (e.g. the conve-

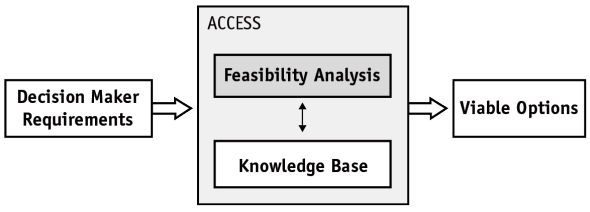

Figure 1: The ACCESS decision support framework.

nience feature includes multiple metrics). Therefore, we adopt the 25 features used by Bonneau et al. [1] in their review. To increase granularity, we define 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). Additionally, we distinguish between additive and selective features. For selective features, only one sub-feature can be assigned to an authentication scheme at any time. For additive features, an authentication scheme can be assigned multiple sub-features.

2.2 Specifying Decision Maker Requirements

Despite being well aware of the text password's problems, decision makers frequently choose this traditional option. Renaud et al. [4] identify as reason the complexity of weighing all viable authentication schemes. Therefore, we aim to render the specification of the requirements for the decision makers as effortless as possible, even in cases where the decision makers might be able to give only an incomplete specification of their requirements. 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). 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. Single sub-features can be selected as hard constraints making them mandatorily required by suitable schemes. The exact handling of selected and unselected features is described in [3]. Figure 2 depicts the specification of requirements.

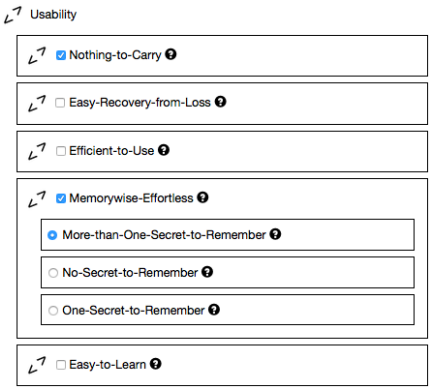

Figure 2: An excerpt of the interface for the specification of decision maker requirements through a (partial) ranking of features. The feature memorywise-effortless shows the specification of hard constraints using sub-features.

2.3 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 represents an instantiation of the multiple criteria evaluation problem: it supports multiple decision criteria (given by the decision maker requirements) and a finite number of potential solutions (given by the authentication schemes). The analytic hierarchy process (AHP) [5] 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. Due to space constraints, we omit a description of AHP, but a brief summary can be found in [3]. We needed to adapt the AHP for its use in the feasibility analysis to address multiple challenges. Due to space considerations, we will discuss only the most significant adaptation: the division of AHP into an expert part and a decision maker part. All other adaptations can be found in [3].

In its conventional form, the AHP serves decision makers to structure their knowledge regarding decisions to be taken. 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 solutions. The challenge is therefore to augment AHP by authentication expert knowledge.

We address this challenge by dividing the AHP into two parts: (1) the first part is to be executed by the decision makers (using the technique explained in the last section), and (2) the second part is to be executed by authentication experts. The definition of the decision problem as well as the construction of the decision hierarchy are static for all authentication scheme decision problems. Additionally, the pairwise comparison of authentication schemes along their features is not influenced by the decision makers' requirements. Therefore, the comparisons are conducted by authentication experts. The decision makers need to provide their requirements only prior to the last AHP step.

3. ACCESS TO INFORMATION IN THE KNOWLEDGE BASE

The first module going beyond the feature set of the existing prototype outlined in the last section is to make the knowledge about text passwords and their alternatives available to decision makers and researchers in a systematic way. Our knowledge base includes descriptions for each of the authentication schemes and each of the authentication scheme features as well as the assignments of the features to the schemes. The interface allowing access to this information regarding each authentication scheme is depicted in Figure 3. It provides a short description of the scheme, the category the scheme belongs to and a list of the sub-features assigned to the scheme.

The interface to access the information regarding the authentication scheme features provides a description of the feature analogously to the authentication schemes and the AHP matrix as an overview of the pairwise comparisons with respect to each of the schemes. Figure 4 depicts the interface used to present the information associated with the features.

4. COLLABORATION FEATURES

The third module of our collaborative authentication research platform are the eponymous collaboration features. One of the key aspects of collaborative work is to allow everyone to contribute their knowledge and experience to achieve the best possible result. Therefore, a discussion feature is deeply entrenched into our platform design. Two types of contributions to a discussion can be made: (a) a comments for general discussions about the authentication

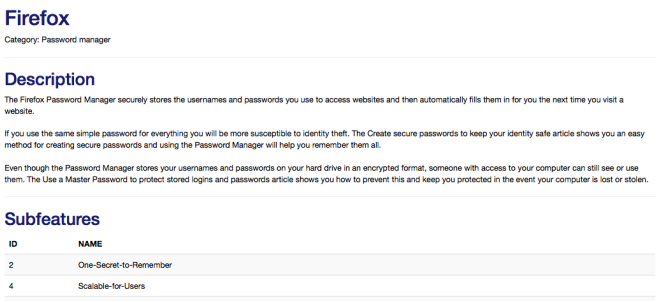

Figure 3: The presentation of the information on each authentication scheme in the knowledge base. The list of associated sub-features is not shown in its entirety due to space considerations.

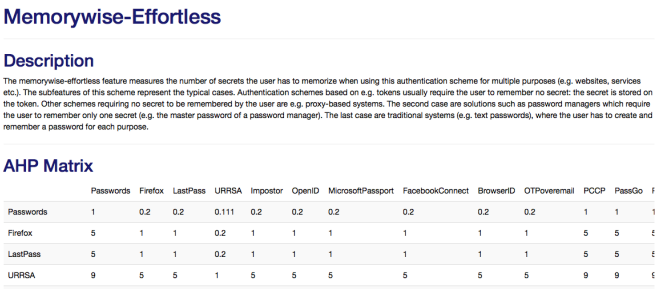

Figure 4: The presentation of the information on each authentication scheme feature.

scheme, and (b) suggestions regarding changes to the knowledge base. Thereby, suggestions can be accepted or rejected. Figure 5 depicts two suggestion threads in a discussion.

In order to allow contributions to the knowledge base from every authentication expert who supports our vision of an open platform providing systematic access to authentication schemes and their features, the discussion feature is open to anyone who registers at the platform. However, beside the general users, the design of our platform includes two additional types of users: moderators and administrators. Normal users can be assigned the moderator role for any feature or authentication scheme. Only users being very familiar with the feature or authentication scheme should be assigned this role, since it allows them to accept or reject suggestions and close threads in the discussions as well as revise the description of the feature or scheme moderated by them. The moderator role is assigned by the administrator, which can edit users and has in general access to all functions of the platform. The full implementation of the moderator role is still in progress.

5. CONCLUSION

In this work, we presented the current progress of expanding our prototype decision support system for choosing suitable authentication schemes into a collaborative authentication research platform. We described the platform's three modules: (a) the integrated decision support system, (b) systematic access to the information in the knowledge base, and (c) the collaborative discussion and suggestion features. We believe that this platform is an important step forward in the systematisation of available knowledge in the authentication research domain, making it available to decision makers and developers of software and services.

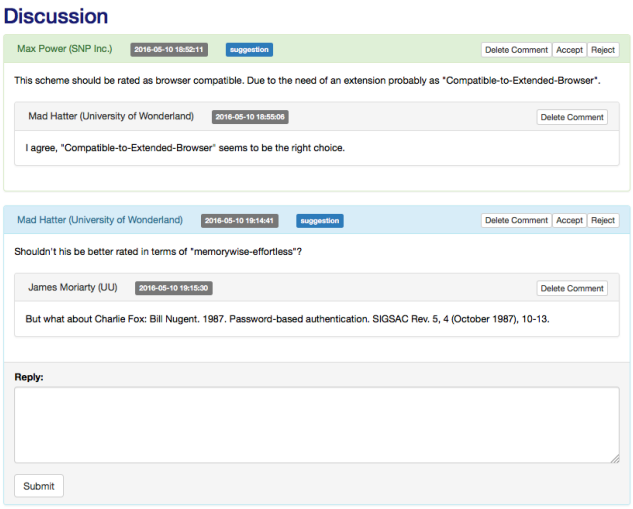

Figure 5: The discussion feature of our platform as seen from the administrators point of view. The figure shows two suggestion threads (one closed, marked in green; on on-going, marked in blue).

6. ACKNOWLEDGEMENTS

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

[1] J. Bonneau, F. Stajano, P. C. van Oorschot, and C. Herley. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE Symposium on Security and Privacy (SP)*, pages 553–567, 2012.

[2] C. Herley and P. Van Oorschot. A research agenda acknowledging the persistence of passwords. *Security & Privacy, IEEE*, 10(1):28–36, 2012.

[3] P. Mayer, S. Neumann, D. Storck, and M. Volkamer. Supporting Decision Makers in Choosing Suitable Authentication Schemes. In *International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, 2016.

[4] K. Renaud, M. Volkamer, and J. Maguire. ACCESS: Describing and Contrasting Authentication Mechanisms. In *Human Aspects of Information Security, Privacy, and Trust*, pages 183–194. Springer, 2014.

[5] T. L. Saaty. *What is the analytic hierarchy process?* Springer, 1988.