ACCESSv2: A Collaborative Authentication Research and Decision Support Platform

Peter Mayer[⋆†], Philip Stumpf[†], Thomas Weber[†], Melanie Volkamer[⋆†]
[⋆] Karlsruhe Institute of Technology (KIT)
[†] Technische Universität Darmstadt
{peter.mayer,melanie.volkamer}@kit.edu

ABSTRACT

In addition to the ubiquitous text password a great variety of other authentication schemes have been proposed. Yet, only very few of the alternatives find their way to practical application. It has been proposed to support decision makers when choosing the most suitable scheme for their application scenario, thereby fostering the adoption of alternatives. In this paper we present ACCESSv2, a collaborative authentication research and decision support platform. It comprises three modules: (1) an information module, which holds and enables access to systematised information about available authentication schemes, (2) a decision support module, that helps decision makers and developers to choose the most suitable scheme for their application scenario, and (3) a collaboration module, which allows experts to contribute to the information module's knowledge base.

1. INTRODUCTION

Despite a unanimous desire by researchers, users, developers and decision makers alike to replace the text password, it remains prevalent [3]. According to Renaud et al. [5] 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 used in practice. To address this issue, Renaud et al. [5] proposed the ACCESS (Authentication ChoiCE Support System) framework. In previous work [4], we presented the first concrete prototype implementation of ACCESS: we built a knowledge base from the results of a literature review, introduced a technique for decision makers to specify their requirements effortlessly, and described the realisation of ACCESS's feasibility analysis using an adapted Analytic Hierarchy Process (AHP).

In this work we present ACCESSv2, the full realisation of our vision outlined in [4]: a collaborative authentication research and decision support platform, where authentication experts can add their knowledge, challenge standing assessments of the reviewed literature, and add further authentication schemes. ACCESSv2 provides three modules: (1) an information module, which holds and enables access to the information about available authentication schemes, (2) a decision support module, which helps decision makers and developers to choose the most suitable scheme for their application scenario, and (3) a collaboration module, which allows anyone to contribute to the information module's knowledge base. In the remainder of this paper, we describe ACCESSv2 and each of its three modules.

2. THE ACCESSV2 PLATFORM

ACCESSv2 is a collaborative authentication research and decision support platform. Its goals are threefold:

G1: Offer a systematic way to access information about available authentication schemes.

G2: Enable non-authentication experts like decision makers or developers to choose suitable authentication schemes.

G3: Enable collaboration through discussions and the suggestion of additions or updates to the information available on the platform.

Each of these goals is implemented in a dedicated module (see Figure 1). All of ACCESSv2's modules were developed according to the User-Centred Design approach [2]. Thus, during development potential users were asked to perform tasks on the platform and give feedback on its current state. These feedback sessions were held in an informal setting and the think-aloud technique was used. This helped to improve

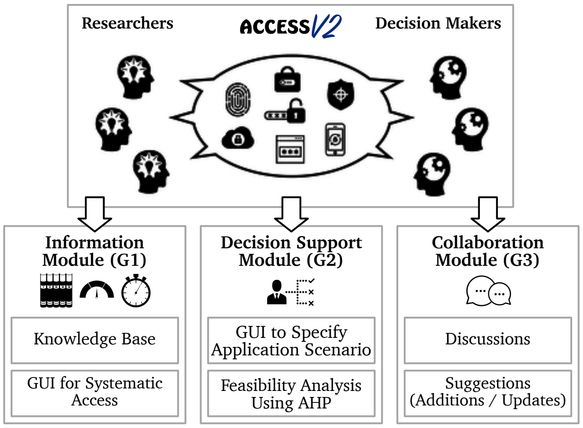

Researchers
ACCESS V2
Decision Makers
Information Module (G1)
Decision Support Module (G2)
Collaboration Module (G3)
Knowledge Base
GUI for Systematic Access
GUI to Specify Application Scenario
Feasibility Analysis Using AHP
Discussions
Suggestions (Additions / Updates)

Figure 1: ACCESSv2 and its three modules.

Who are you? Adventures in Authentication Workshop 2018.
August 12–14, 2018, Baltimore, MD, USA.

the platform in several aspects (e.g. workflows, understandability of available options, etc.). While the concepts of ACCESSv2 are based on the prototype implementation described in [4], it has been completely redeveloped and offers much more functionality. The prototype comprised only two components: a static knowledge base with hardcoded information about authentication schemes and a basic interface for the decision support. All of ACCESSv2's components have been developed from the ground up with the feedback we received during the feedback sessions. ACCESSv2 is open source software available at GitHub[1] and it can be freely used by anyone online[2]. In the following sections, its three modules will be described in detail.

3. INFORMATION MODULE

The first of the platform's modules is the information module. It allows accessing information about authentication schemes in a systematic way (i.e. it implements **G1**) and is comprised of the *knowledge base* holding the information about the authentication schemes and the *GUI to access this information* in a systematic manner.

3.1 Knowledge Base

Bonneau et al. [1] present a review of 36 authentication schemes of various categories. 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 (details in [4]). The overall number of schemes included in our knowledge base is 45.

The authentication scheme features defined by the original ACCESS framework [5] remain abstract and difficult to measure (e.g. the convenience feature includes multiple metrics). Thus, we adopt the 25 features used in Bonneau et al.'s review [1]. To increase granularity, we defined 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*). We distinguish between additive (an authentication scheme can be assigned multiple sub-features) and selective (only one sub-feature can be assigned to an authentication scheme at any time) features. The details of this refinement can be found in [4].

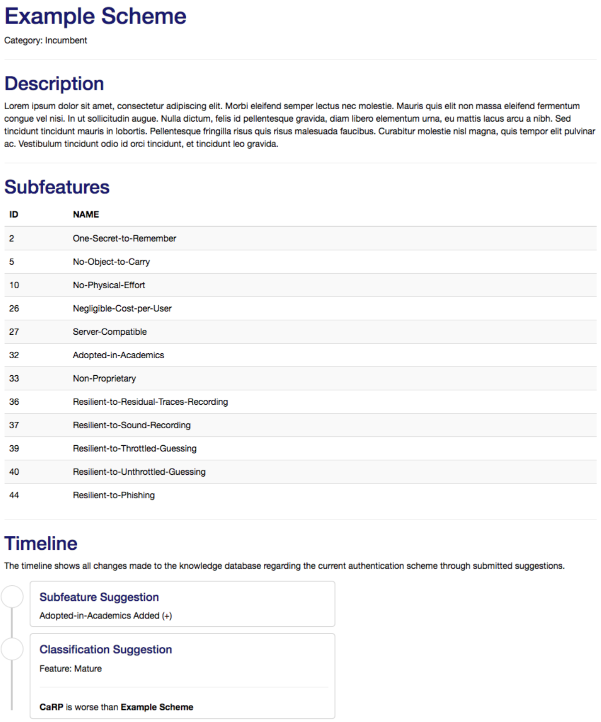
In ACCESSv2 the aforementioned information is stored in a dynamic database structure in order to enable the functionality of the collaboration module.

3.2 GUI for Systematic Access to Information

The information module's GUI allows accessing the information stored in the knowledge base in a systematic manner (see Figure 2). It provides 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. It also shows a timeline of the changes made to the knowledge base over time and thereby allows retracing how an authentication scheme's evaluation has changed.

4. DECISION SUPPORT MODULE

The decision support module enables non-authentication experts like decision makers and developers to choose suitable authentication schemes for their specific application scenarios (i.e. it implements **G2**). To that end ACCESSv2 offers an *interface* which first guides the decision maker through the specification of their application scenario's requirements and displays the most suitable schemes which are calculated according to a *feasibility analysis*.



Example Scheme

Category: Incumbent

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eleifend semper lectus nec molestie. Mauris quis elit non massa eleifend fermentum congue vel nisi. In ut sollicitudin augue. Nulla dictum, felis id pellentesque gravida, diam libero elementum urna, eu mattis lacus arcu a nibh. Sed tincidunt tincidunt mauris in lobortis. Pellentesque fringilla risus quis risus malesuada faucibus. Curabitur molestie nisl magna, quis tempor elit pulvinar ac. Vestibulum tincidunt odio id orci tincidunt, et tincidunt leo gravida.

Subfeatures

ID	NAME
2	One-Secret-to-Remember
5	No-Object-to-Carry
10	No-Physical-Effort
26	Negligible-Cost-per-User
27	Server-Compatible
32	Adopted-in-Academics
33	Non-Proprietary
36	Resilient-to-Residual-Traces-Recording
37	Resilient-to-Sound-Recording
39	Resilient-to-Throttled-Guessing
40	Resilient-to-Unthrottled-Guessing
44	Resilient-to-Phishing

Timeline

The timeline shows all changes made to the knowledge database regarding the current authentication scheme through submitted suggestions.

Subfeature Suggestion

Adopted-in-Academics Added (+)

Classification Suggestion

Feature: Mature

CaRP is worse than **Example Scheme**

Figure 2: The interface displaying the information about the authentication schemes.

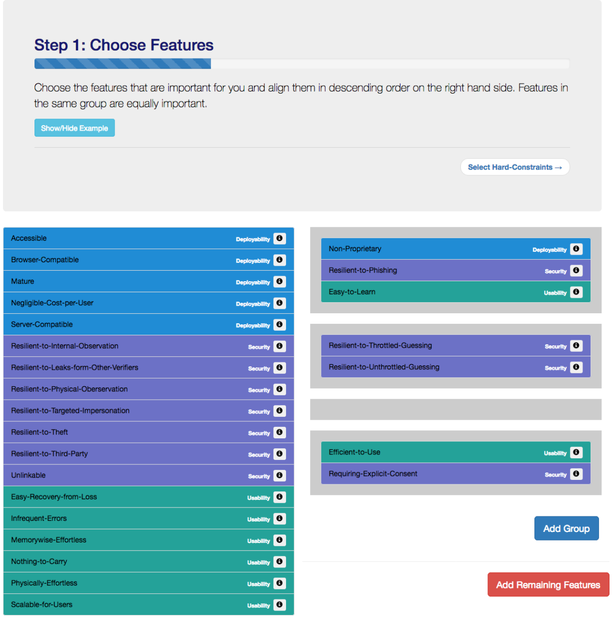
4.1 Interface for the Specification of the Application Scenario and Results Display

Our goal in designing the interface for the specification of the application scenario was to render the specification 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. To achieve this, we designed an interface which guides decision makers through the process of specifying the requirements of their application scenario in two steps.

First, the decision makers have to (partially) rank features to specify their relative importance (see Figure 3). Each feature can be individually selected and dragged from the list of available features on the left rightwards to the list of features considered in the feasibility analysis. In the left list, features are grouped according to their importance in the application scenario. The further to the top a group is placed by the decision maker, the higher is its importance (and the higher the weighting in the feasibility analysis).

Then, in the second step, the decision maker can select hard constraints (i.e. mandatorily required sub-features). Figure 4 depicts this interface. These hard constraints can be specified as conjunctions (e.g. *Resilient-to-Throttled-Guessing* AND *Resilient-to-Unthrottled-Guessing*), as disjunctions (e.g.

[1] https://github.com/SECUSO/ACCESSv2
[2] https://access.secuso.org/



Step 1: Choose Features

Choose the features that are important for you and align them in descending order on the right hand side. Features in the same group are equally important.

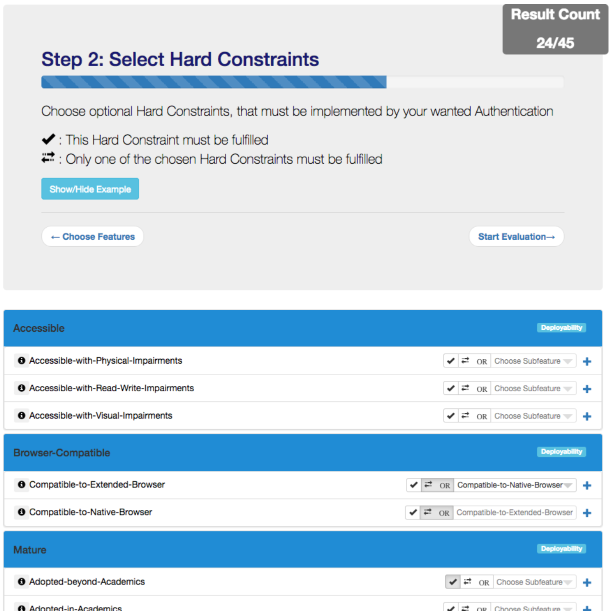
Accessible Deployability
Browser-Compatible Deployability
Mature Deployability
Negligible-Cost-per-User Deployability
Server-Compatible Deployability
Resilient-to-Internal-Observation Security
Resilient-to-Leaks-form-Other-Verifiers Security
Resilient-to-Physical-Oberservation Security
Resilient-to-Targeted-Impersonation Security
Resilient-to-Theft Security
Resilient-to-Third-Party Security
Unlinkable Security
Easy-Recovery-from-Loss Usability
Infrequent-Errors Usability
Memorywise-Effortless Usability
Nothing-to-Carry Usability
Physically-Effortless Usability
Scalable-for-Users Usability

Non-Proprietary Deployability
Resilient-to-Phishing Security
Easy-to-Learn Usability

Resilient-to-Throttled-Guessing Security
Resilient-to-Unthrottled-Guessing Security

Efficient-to-Use Usability
Requiring-Explicit-Consent Security

Figure 3: The interface used to rank the available features with respect to their importance in the application scenario. On the left is the list of the available features. These can be dragged to the right into the list of features considered in the feasibility analysis. Features are always grouped on the right. The features in each group (grey boxes) are considered as equally important during the feasibility analysis. Empty groups are ignored.



Step 2: Select Hard Constraints

Result Count 24/45

Choose optional Hard Constraints, that must be implemented by your wanted Authentication

✓ : This Hard Constraint must be fulfilled
⇄ : Only one of the chosen Hard Constraints must be fulfilled

Accessible Deployability
Accessible-with-Physical-Impairments ✓ ⇄ OR Choose Subfeature +
Accessible-with-Read-Write-Impairments ✓ ⇄ OR Choose Subfeature +
Accessible-with-Visual-Impairments ✓ ⇄ OR Choose Subfeature +

Browser-Compatible Deployability
Compatible-to-Extended-Browser ✓ ⇄ OR Compatible-to-Native-Browser +
Compatible-to-Native-Browser ✓ ⇄ OR Compatible-to-Extended-Browser +

Mature Deployability
Adopted-beyond-Academics ✓ ⇄ OR Choose Subfeature +
Adopted-in-Academics ✓ ⇄ OR Choose Subfeature +

Figure 4: Excerpt of the interface used to specify hard constraints. In this example the specified constraints are: *Adopted-beyond-Academics* AND (*Compatible-to-Native-Browser* OR *Compatible-to-Extended-Browser*). Authentication schemes not meeting the hard constraints are excluded from the results of the feasibility analysis. The counter in the upper right corner gives immediate feedback on how many schemes are meeting the requirements.

Non-Proprietary OR *Server-Compatible*), or as a combination thereof (e.g. *Resilient-to-Throttled-Guessing* AND (*Non-Proprietary* OR *Server-Compatible*)). A counter in the right hand corner of the interface always gives immediate feedback to the decision maker on how many authentication schemes fulfil the specified hard constraints.

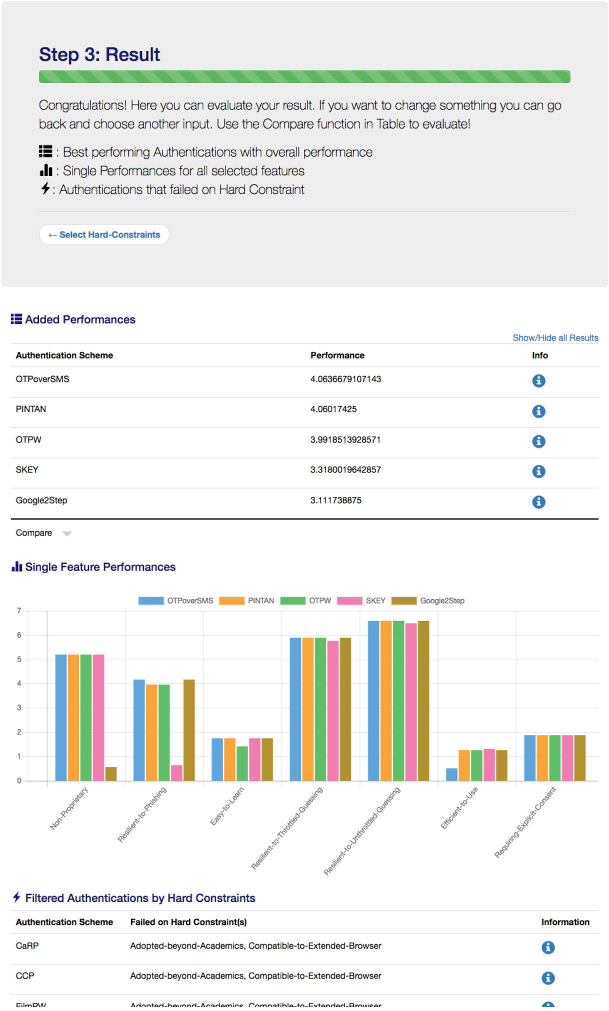
In both of the aforementioned steps, explanations for each feature and sub-feature are available to the decision maker. Also, both steps include graphical instructions with examples on how to use the interface. These instructions can be accessed through a *Show/Hide Example*-button.

Upon completion of the two steps, the decision maker can advance to the interface displaying the results. The feasibility analysis (see next section) determining the most suitable schemes is performed in the background. The results interface (see Figure 5) displays by default a list of the five most suitable schemes with their suitability ranking (according to the feasibility analysis). However, it is possible to show the rankings of all schemes meeting the hard constraints by clicking the provided *show all*-button. In order to enable decision makers to look up additional information for the most suitable schemes, each entry in the list has a button linking it directly to the respective authentication scheme's page in the information module. Additionally, the interface allows comparing scores even for the authentication schemes which were excluded due to hard-constraints. Below the list of suitable authentication schemes, the interface displays graphical rankings of the schemes for each of the features selected in the first step, allowing a finer grained comparison along the features deemed important for the application scenario. Finally, below the rankings for each feature, the decision maker can find the list of authentication schemes which were excluded due to hard constraints.

4.2 Feasibility Analysis

Based on the decision maker requirements, the feasibility analysis identifies the most suitable authentication schemes among those available in ACCESSv2's 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) [6] is an established approach to solving such problems. It is particularly well suited for ACCESSv2 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. We needed to adapt the AHP for its use in the feasibility analysis to address multiple challenges. Due to space constraints, we omit the description of AHP and the adaptations. More information on both topics can be found in [4].

However, for ACCESSv2, one further enhancement was introduced into the feasibility analysis in comparison to the prototype implementation in [4]: the possibility to exclude features from the feasibility analysis. Where before the "unnecessary" features were simply ranked last, they are now completely left out of the feasibility analysis.



Step 3: Result

Congratulations! Here you can evaluate your result. If you want to change something you can go back and choose another input. Use the Compare function in Table to evaluate!

☰ : Best performing Authentications with overall performance
📊 : Single Performances for all selected features
⚡: Authentications that failed on Hard Constraint

← Select Hard-Constraints

☰ Added Performances

Show/Hide all Results

Authentication Scheme	Performance	Info
OTPoverSMS	4.0636679107143	ℹ
PINTAN	4.06017425	ℹ
OTPW	3.9918513928571	ℹ
SKEY	3.3180019642857	ℹ
Google2Step	3.111738875	ℹ

Compare

📊 Single Feature Performances

⚡ Filtered Authentications by Hard Constraints

Authentication Scheme	Failed on Hard Constraint(s)	Information
CaRP	Adopted-beyond-Academics, Compatible-to-Extended-Browser	ℹ
CCP	Adopted-beyond-Academics, Compatible-to-Extended-Browser	ℹ
FilmPW	Adopted-beyond-Academics, Compatible-to-Extended-Browser	ℹ

Figure 5: Excerpt of the interface displaying the results according to the rankings specified in figure 3 and the hard constraints specified in figure 4.

5. COLLABORATION MODULE

The collaboration module implements **G3**: it allows experts to discuss and suggest changes (additions and updates) of the available information in the knowledge base, thereby collaboratively enhancing the platform's contents. Two types of collaborative contributions can be made: (1) *general discussions* regarding an authentication scheme or feature, and (2) specific *suggestions* for changes to the knowledge base. To facilitate the collaboration, two types of users exist in ACCESSv2: normal users and administrators. In addition to contributing in the two aforementioned ways, administrators can mediate the collaboration by accepting or rejecting suggestions and closing threads in the general discussions. Additionally, they can revise the descriptions of the features and authentication schemes should the need arise.

5.1 General Discussions

General discussions are meant for the exchange of information about authentication schemes that goes beyond the features in the knowledge base. The original proposal of ACCESS already envisioned the possibility to provide feedback on deployments of authentication schemes. However, where and with how many users a scheme has been deployed might go beyond the *Mature*-feature. This information could, for instance, be collected in the general discussions.

5.2 Suggestions

Authentication experts can suggest changes to the knowledge base (i.e. additions and updates) when new research becomes available. Three types of changes can be proposed: (1) adding new authentication schemes, (2) adding or removing a sub-feature from an authentication scheme, and (3) rating an authentication scheme differently within an equivalence class of a feature (see [4] for details). Each suggestion is supported through a dedicated interface.

The addition of new authentication schemes is a three-step process. In the first step, the basic data of the scheme has to be entered (see Figure 6). The second step is the specification of the fulfilled sub-features (see Figure 7). In the third step, the new authentication scheme has to be pairwise compared regarding each feature to each of the other authentication schemes in the same equivalence class, i.e. whether it performs worse, equal, or better (see Figure 8, more details regarding the equivalence classes can be found in [4]). Upon completion of the three steps, the suggestion is available for review by administrator users, who can accept the addition to the knowledge base, reject it or modify it in case of small errors. Once the addition is accepted, it is immediately available in the decision support module.

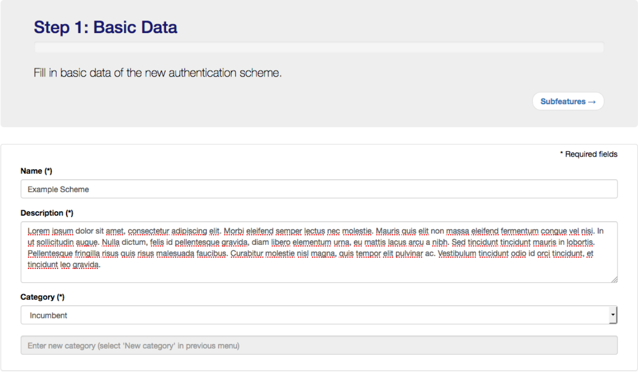
To suggest the addition or removal of a sub-feature for an authentication scheme already present in the knowledge base, a variation of the same interface as used in the second step of the addition of a new scheme is utilised. It allows the user to add or remove exactly one sub-feature and submit this change as suggestion. Likewise, changing an authentication scheme's rating in an equivalence class can be suggested using a variation of the interface utilised during the third step of the addition of a new scheme. Both variations also include the possibility to justify the suggestions in text and include publications the suggestion is based on. All suggestions are added as discussion threads to the authentication scheme's page in the information module. Other users can comment on the suggestions and administrators can accept or reject the changes. Figure 9 depicts the interface of an open suggestion as displayed on the information module page.

Analogously to the decision support module, explanations for the features and sub-features, and authentication schemes are available to the user as tooltips (see Figure 7).

6. CONCLUSION AND FUTURE WORK

In this work, we presented ACCESSv2, a collaborative authentication research and decision support platform. We described the platform's three modules: (1) an information module, which holds and enables access to the information about available authentication schemes, (2) a collaboration module, which allows anyone to contribute to the information module's knowledge base, and (3) a decision support module, which helps decision makers and developers to choose the most suitable authentication scheme for their application scenario.

ACCESSv2 has already been successfully used by independent decision makers in an academic project on user-friendly



Step 1: Basic Data

Fill in basic data of the new authentication scheme.

Subfeatures →

* Required fields

Name (*)

Example Scheme

Description (*)

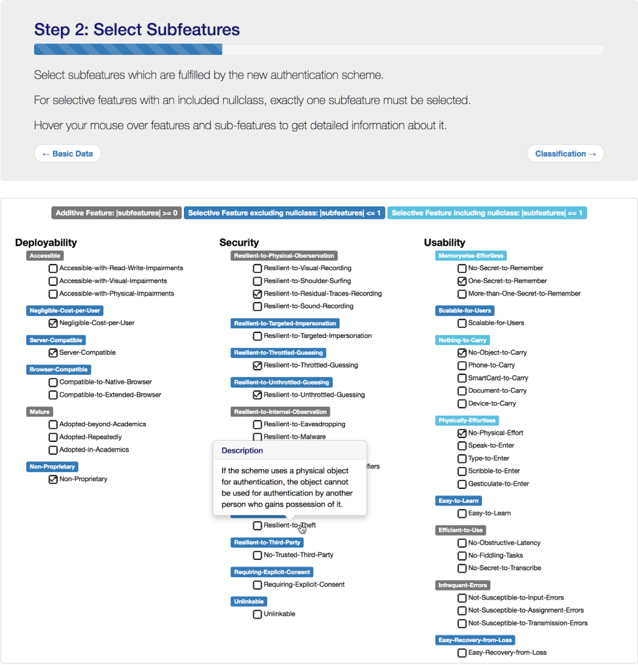
Lorem ipsum dolor sit amet, consectetur adipiscing elit. Morbi eleifend semper lectus nec molestie. Mauris quis elit non massa eleifend fermentum congue vel nisi. In ut sollicitudin augue. Nulla dictum, felis id pellentesque gravida, diam libero elementum urna, eu mattis lacus arcu a nibh. Sed tincidunt tincidunt mauris in lobortis. Pellentesque fringilla risus quis risus malesuada faucibus. Curabitur molestie nisl magna, quis tempor elit pulvinar ac. Vestibulum tincidunt odio id orci tincidunt, et tincidunt leo gravida.

Category (*)

Incumbent

Enter new category (select 'New category' in previous menu)

Figure 6: Interface used in the first step of the suggestion of new authentication schemes.



Step 2: Select Subfeatures

Select subfeatures which are fulfilled by the new authentication scheme.

For selective features with an included nullclass, exactly one subfeature must be selected.

Hover your mouse over features and sub-features to get detailed information about it.

← Basic Data

Classification →

Additive Feature: |subfeatures| >= 0

Selective Feature excluding nullclass: |subfeatures| <= 1

Selective Feature including nullclass: |subfeatures| == 1

Deployability

Accessible
- ☐ Accessible-with-Read-Write-Impairments
- ☐ Accessible-with-Visual-Impairments
- ☐ Accessible-with-Physical-Impairments

Negligible-Cost-per-User
- ☑ Negligible-Cost-per-User

Server-Compatible
- ☑ Server-Compatible

Browser-Compatible
- ☐ Compatible-to-Native-Browser
- ☐ Compatible-to-Extended-Browser

Mature
- ☐ Adopted-beyond-Academics
- ☐ Adopted-Repeatedly
- ☐ Adopted-in-Academics

Non-Proprietary
- ☑ Non-Proprietary

Security

Resilient-to-Physical-Oberservation
- ☐ Resilient-to-Visual-Recording
- ☐ Resilient-to-Shoulder-Surfing
- ☑ Resilient-to-Residual-Traces-Recording
- ☐ Resilient-to-Sound-Recording

Resilient-to-Targeted-Impersonation
- ☐ Resilient-to-Targeted-Impersonation

Resilient-to-Throttled-Guessing
- ☑ Resilient-to-Throttled-Guessing

Resilient-to-Unthrottled-Guessing
- ☑ Resilient-to-Unthrottled-Guessing

Resilient-to-Internal-Observation
- ☐ Resilient-to-Eavesdropping
- ☐ Resilient-to-Malware

fiers

Description

If the scheme uses a physical object for authentication, the object cannot be used for authentication by another person who gains possession of it.

- ☐ Resilient-to-Theft

Resilient-to-Third-Party
- ☐ No-Trusted-Third-Party

Requiring-Explicit-Consent
- ☐ Requiring-Explicit-Consent

Unlinkable
- ☐ Unlinkable

Usability

Memorywise-Effortless
- ☐ No-Secret-to-Remember
- ☑ One-Secret-to-Remember
- ☐ More-than-One-Secret-to-Remember

Scalable-for-Users
- ☐ Scalable-for-Users

Nothing-to-Carry
- ☑ No-Object-to-Carry
- ☐ Phone-to-Carry
- ☐ SmartCard-to-Carry
- ☐ Document-to-Carry
- ☐ Device-to-Carry

Physically-Effortless
- ☑ No-Physical-Effort
- ☐ Speak-to-Enter
- ☐ Type-to-Enter
- ☐ Scribble-to-Enter
- ☐ Gesticulate-to-Enter

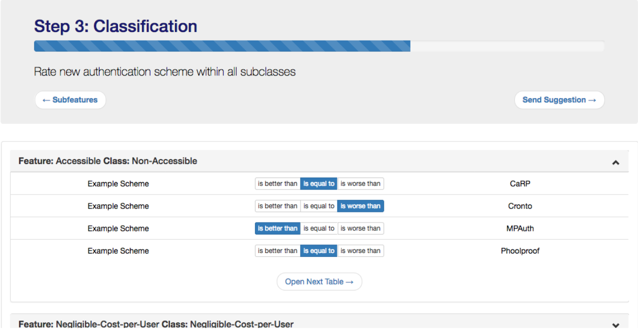
Easy-to-Learn
- ☐ Easy-to-Learn

Efficient-to-Use
- ☐ No-Obstructive-Latency
- ☐ No-Fiddling-Tasks
- ☐ No-Secret-to-Transcribe

Infrequent-Errors
- ☐ Not-Susceptible-to-Input-Errors
- ☐ Not-Susceptible-to-Assignment-Errors
- ☐ Not-Susceptible-to-Transmission-Errors

Easy-Recovery-from-Loss
- ☐ Easy-Recovery-from-Loss

Figure 7: Interface used in the second step of the suggestion of new authentication schemes. Tooltips provide additional information all three steps.



Step 3: Classification

Rate new authentication scheme within all subclasses

← Subfeatures

Send Suggestion →

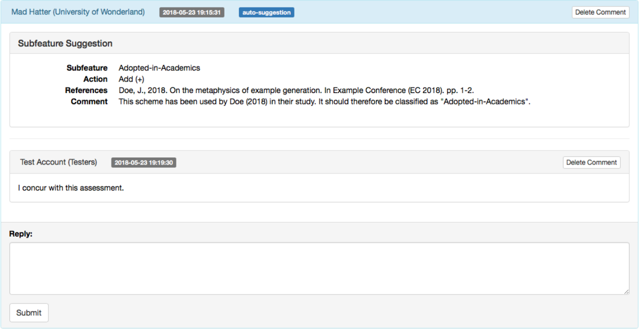
Feature: Accessible **Class:** Non-Accessible

Example Scheme	is better than [✓ is equal to] is worse than	CaRP
Example Scheme	is better than is equal to [✓ is worse than]	Cronto
Example Scheme	[✓ is better than] is equal to is worse than	MPAuth
Example Scheme	is better than [✓ is equal to] is worse than	Phoolproof

Open Next Table →

Feature: Negligible-Cost-per-User **Class:** Negligible-Cost-per-User

Figure 8: Interface used in the third step of the suggestion of new authentication schemes.



Mad Hatter (University of Wonderland) 2018-05-23 19:15:31 auto-suggestion

Delete Comment

Subfeature Suggestion

Subfeature	Adopted-in-Academics
Action	Add (+)
References	Doe, J., 2018. On the metaphysics of example generation. In Example Conference (EC 2018). pp. 1-2.
Comment	This scheme has been used by Doe (2018) in their study. It should therefore be classified as "Adopted-in-Academics".

Test Account (Testers) 2018-05-23 19:19:30

Delete Comment

I concur with this assessment.

Reply:

Submit

Figure 9: An open suggestion to add a sub-feature to an authentication scheme. Users can discuss the suggestion.

authentication and encryption to choose a suitable authentication scheme. We invite everyone to try ACCESSv2 and hope to spark discussions among authentication experts, decision makers, and developers. We believe that ACCESSv2 is an important step forward in the systematisation of available knowledge in the authentication research domain.

An important part of future work remains extending and continuously updating the knowledge base with new authentication schemes and new research results. Another area for future work are extensions of the information module with more information relevant for developers, e.g. available libraries, implementations, or information regarding the integration of the schemes into products and services. Last but not least, a formal evaluation of ACCESSv2 might uncover further areas for future improvements.

7. ACKNOWLEDGEMENT

This work was supported by the German Federal Ministry of Education and Research in the Competence Center for Applied Security Technology (KASTEL).

8. 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] J. Gulliksen, B. Göransson, I. Boivie, S. Blomkvist, J. Persson, and Å. Cajander. Key principles for user-centred systems design. *Behaviour & Information Technology*, 22(6):397–409, Nov. 2003.

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

[4] P. Mayer, S. Neumann, D. Storck, and M. Volkamer. Supporting Decision Makers in Choosing Suitable Authentication Schemes. In *International Symposium of Human Aspects of Information Security Assurance*, pages 67–77, 2016.

[5] 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. 2014.

[6] T. L. Saaty. *What is the analytic hierarchy process?* 1988.