ACCESS: Describing and Contrasting Authentication Mechanisms

Karen Renaud[1], Melanie Volkamer[2], Joe Maguire[1]

[1] School of Computing Science, University of Glasgow,
{karen.renaud,joseph.maguire}@glasgow.ac.uk
[2] Technische Universität Darmstadt, CASED, Germany,
melanie.volkamer@cased.de

Abstract. The password the almost universal authentication solution yet is buckling under the strain. It demonstrates insufficiency and weakness due to poor choice, reuse and ease of sharing Graphical passwords, biometrics, and hardware tokens have been proposed as alternatives. However, industry has not embraced these alternatives. One possible explanation is the complexity of the choice process, i.e. for which situation and which person which alternative is most appropriate. To support authentication decision-markers in this process we suggest a framework called ACCESS (**A**uthentication **C**hoi**CE** **S**upport **S**ystem) which captures situation and user related requirements, consults a knowledge base of existing authentication mechanisms and their properties, and suggests those mechanisms that match the specified requirements.

1 Introduction

The password can provide a high theoretical security, but the security level in practice is compromised by password reuse, use of simple passwords, and recording of passwords [1]. Strict rules for password creation cannot mitigate against human frailty so it seems wise to consider more usable alternatives with less cognitive load such as graphical passwords [2–4], biometrics [5–8], hardware tokens [9], two/multi-factor authentication [10]. and single sign-on solutions such as OpenID [11].

It is strange that passwords are still so ubiquitous in the light of this range of viable alternatives. It seems to run counter to the natural order of things for an inferior technology to prevail. On the other hand, this level of caution is understandable since authentication is essentially a risk mitigation technique, and organisations have to satisfy their auditors. Passwords are a well-established technique with provable theoretical strength, while alternatives remain an unknown quantity. A few papers have started to emerge [12, 13] which specifically address the strengths of some of these alternatives, but these are unlikely to make an impact on industry in their present format.

As things stand, developers and authentication decision makers are probably not convinced of the effectiveness of password alternatives as access control mechanisms. The academic literature is most likely too obscure and unrealistic

to convince them. Successful use of alternatives by their contemporaries is likely to carry more weight and might convince them [14, 15], but no one of a high enough profile has, thus far, taken the plunge. One gets the sense that industry is watching the effects of Apple's recent use of fingerprint biometrics for their iPhone 5S phone very carefully, and this might well be exactly what will make the difference. However, biometrics, while undeniably useful for single owner devices, is not going to be tenable in many a corporate setting.

It might be time for some kind of pro-active intervention, a way to support decision-makers in selecting an appropriate authentication mechanism. The idea would be make it easy for decision makers to access the facts about alternatives, to find answers to their questions and to address their concerns. We propose a framework called ACCESS (**A**uthentication **C**hoi**CE** **S**upport **S**ystem) to capture requirement specifications from decision-makers, consult a knowledge base of existing authentication mechanism properties, and suggest mechanisms that meet the specified requirements both wrt. the concrete situation and user group in mind.

Our *first contribution* is the description of this framework. Our *second contribution* is to identify categories of requirements that will feed into ACCESS based on a literature review in the areas of technology adoption and acceptance, security, usable security, marketing and economics. To confirm these, we conducted a survey with current developers in the field, i.e. target users of ACCESS, to confirm our requirement categories.

As future work, the knowledge base will be created based on existing literature and, where necessary, additional investigations and evaluations of existing proposals carried out to ensure that the knowledge-base supporting ACCESS does indeed deliver value. The remainder of this paper is organised as follows: We first present our proposal for the ACCESS framework to support developers who are interested in considering alternative authentication. The following section presents the results of our literature review: a set of requirements. We then present, in Section 4, the results of an online survey we conducted with developers. We then give an example of how ACCESS might be used before concluding.

2 ACCESS Framework

ACCESS is a decision maker support framework, which encodes and encapsulates a wide range of expert knowledge about authentication mechanisms. Such frameworks have been proposed for use in a wide variety of areas [16–19]. and follow three broad approaches [20]. The first is *prior articlulation of preferences* where the decision maker provides a number of requirements, and the framework then ranks the alternatives from its knowledge base in terms of expected utility. The second is *interactive articulation of preferences* where the decision maker interacts with the system, and is asked a number of questions in order to guide the user towards one optimal solution. The third approach is the *posterior artic-*

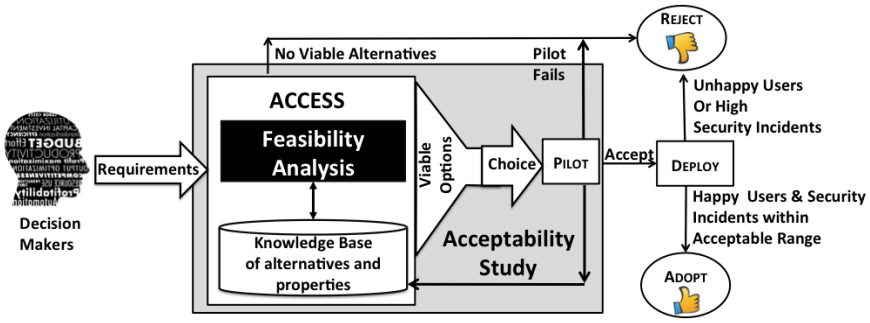

Fig. 1. ACCESS Framework (option 1 according to [20]

ulation of preferences where the system generates a number of solutions without inputs, and presents these to the decision maker who is then makes a choice.

For the design of the ACCESS framework it is important to known that there is a clear difference between *acceptance* and *adoption* while the goal of ACCESS is to adopt alternatives. Acceptance is a first step, which includes identifying a technology (here an alternative authentication mechanism) that meets the decision maker's requirements. Then this technology needs to be piloted. If the piloting is a success, the technology is deployed and carefully monitored to ensure that it performs well. If it does, it might, over time, be adopted into full usage by the company. Without the pilot, it is not even accepted, and since acceptance is a necessary pre-requisite to adoption, no long term usage will ensue.

An overview of the proposed ACCESS framework is shown in Figure 1. The decision maker provides information about the different requirements either at the beginning or during the *Feasibility Assessment*. The feasibility assessment tool uses the *Knowledge Base*, containing descriptive information about a range of authentication mechanisms, to suggest a number of ranked alternatives for consideration. The decision makers would choose one and conduct a *pilot* study with some real users to determine whether the mechanism meets requirements with the context of use. The pilot's outcome is examined and a decision is made as to whether to *deploy* the mechanism in the wild or to reject it. The performance of the mechanism will have to be carefully monitored, producing data on the usage experience and security incidents. Should these results show high levels of security incidents or user dissatisfaction, the alternative authentication method is rejected; otherwise, it is very likely to be *adopted* by the decision makers.

In order to provide an ACCESS tool for decision makers, it is necessary to identify those types of requirements that are relevant in order to select appropriate alternatives for specific situations, services, and users. Once these requirements are identified, the knowledge base can be constructed containing those alternatives proposed in literature together with information about their properties with respect to the identified requirements. It is expected that current evidence available in the literature might well not address all types of requirements. Hence further studies and analyses will be needed to fill the gaps. Furthermore,

it will be necessary to dynamically and continuously keep the knowledge base updated as new attacks emerge and new devices become popular. ACCESS can thereby provide support for decision makers in identifying suitable alternative authentication techniques.

3 Requirement Identification

We conducted a research literature review on adoption, acceptance, security, and usable security, as well as business-related publications in order to identify relevant requirements. We identified four categories of requirements: Risk Mitigation, Quality of Use, User Context, and Business Context. Their relation is illustrated in Figure 2.

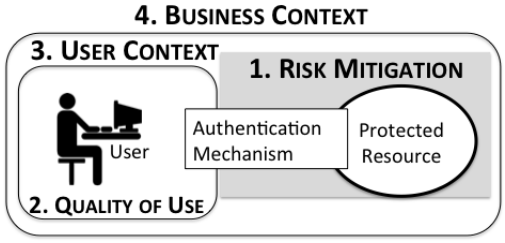

Fig. 2. Users Authenticating

3.1 Risk Mitigation

Authentication is essentially risk mitigation. The value of the protected resource should be matched with the strength of the authentication mechanism being used to protect it. Correspondingly, the framework will need to determine whether the security offered in practise by a particular authentication scheme matches the value of the resource being protected and the assumed attacker capabilities. De Angeli, Coventry, Johnson and Renaud outline in [21] the following dimensions to assess the security of authentication mechanisms and could be used for judging on the risk mitigation level:

Guessability: How easy it is to guess the secret. Note, no universally accepted security rating method currently exists. One measure that is commonly used as a theoretical strength indicator is *theoretical password space*, which is a measure of how many possible passwords (whether textual, graphical, or other) exist given certain constraints on the makeup of the password. Since users tend to choose simple passwords that do not take advantage of the entire possible password space, the theoretical password space is a relatively weak measure of offered security. Unfortunately, the results of previous user studies cannot be used as a substitute for a universal strength measure either.

Observability: The ease with which the entry of the secret can be observed (including shoulder surfing and malicious software on the corresponding device).

Recordability: The ability for an attacker to utilise a user-generated recording, either *of* or *associated with* an authentication secret.

We propose to integrate these into the ACCESS framework. Furthermore, the security of different password recovery mechanisms should be considered. All these aspects are not proposed to be used quantitatively, but they do support a comparison between different schemes, so that the best scheme for a particular context, in terms of risk mitigation, can be identified.

3.2 Quality in Use

The traditional technology acceptance (TAM) model suggests that the most influential factors leading to adoption are *perceived usefulness* and *perceived ease-of-use*, and these certainly confirm the importance of the usability aspect of this requirement category. This is especially important when users are customers rather than employees [22, 23]. Usability testing is routinely carried out during software development [24]. An equally important aspect of quality in use, which is not encapsulated within traditional usability, is convenience [25]. Users routinely choose based on convenience rather than strength [26, 27]. Moreover, we now arguably inhabit a consumer-era where the real power of the market lies with consumers, not with the service providers. An authentication mechanism designed for the mainstream must match customer expectations and represent a balance between costs and benefits *to consumers*. A number of aspects are relevant to quality in use:

Memorability: The need to remember them is the password's chief flaw. Humans generate simple secrets to avoid forgetting [28], and this compromises the mechanism's theoretical strength.

Accessibility: Authentication should be accessible to most individuals, even those with disabilities such as dyslexia, colour blindness or mobility issues so as to ensure that the system meets the needs of the end-users [29]. For example, an authentication mechanism reliant on sentences is not suitable if any of the users are likely to be illiterate or to include a significant number of dyslexics. On the other hand, if literacy is a given, and the target audience is elderly, then the deployed authentication mechanism cannot reasonably rely on perfect memory.

Equipment: Some alternative authentication methods require extra hardware, which may reduce the viability of the mechanism. If the target users are employees, this aspect is easily controlled. If they are customers using their own devices, expectations are far more constrained.

Convenience: The effort associated with authentication must be appropriate for the envisioned use. Three aspects [30] are relevant: **(1) Enrolment Time**: Lengthy enrolment times could deter users but a lengthy enrolment phase may be acceptable if it affords authentication secrets that are used rarely but endure for years. **(2) Authentication Time**: Time-consuming authentication could deter on-going use of an application or service. However, lengthy authentication may be acceptable in high-risk situations or if it reduces inconvenience

in other areas, e.g. password reset. **(3) Replacement Time**: If employees are locked out of their accounts, their inability to do their jobs costs the organisation money. If customers cannot log into a system, they cannot make a purchase. Thus it is important for replacement to be given due consideration.

It is unlikely that the decision-maker will have a specific mandated time span for these activities. What is reasonable though, is to encode the target user group's tolerance for delays in each of these areas. A simple scheme of Low/Medium/High could suffice.

3.3 Business Context

The reality of the current world economy makes the business environment extremely competitive so businesses want to be sure that any new innovation is going to benefit them ie. not lead to extra expense with no benefit to offset the expense. This can be termed *business value*. In terms of switching to an alternative the benefit might be reduced calls to the help desk and increased customer satisfaction. The fundamental monetary costs of an authentication approach can be broadly classified into three types [28], as follows:

User cost: If the authentication approach relies on generic hardware and software, e.g. traditional operation system and keyboards, then there are no real costs for the user. However, if the authentication approach is token or biometric-based then the cost of specialised hardware and software for each user would need to be considered.

Infrastructure cost: The cost for the necessary infrastructure to operate the authentication solution. The infrastructure costs for almost any authentication solution are likely to be high. However, the aim is that as more users embrace a system or application, the infrastructure costs are reduced, as an increase in users squeezes value from infrastructure.

Administration cost: The cost associated with the number of professionals required to manage bureaucracy and effectively operate an authentication solution. This is likely to be directly proportional to the number of users.

It will be challenging to estimate some of these costs accurately so perhaps a granular qualitative scheme should be adopted, which supports comparison between different mechanisms but does not attempt to quantify the actual cost.

3.4 User Context

According to [30], context includes the following aspects which we propose to use in ACCESS:

Anticipated Frequency of Use: A mechanism which is used infrequently has greater memorability requirements.

Platform & Place: The envisioned device and/or software of an authentication mechanism and the envisioned environments where an authentication mechanism will be used. The modern mobile computer or smartphone has pushed powerful computation and access to the Internet, onto many more devices. Hence one cannot make any assumptions about platform or place of use.

Purpose: The *reason* for deploying an authentication mechanism. The mechanism may well serve one purpose in one setting but another, elsewhere. For example, in one setting a person might authenticate to enforce accountability but at other times to authorise purchases.

4 Developer Survey to Confirm Requirements

Having consulted the literature review to identify the requirements relevant to decision making, we noticed that developers are, in general, rarely addressed in the research literature on authentication and technology acceptance and adaption. However, at the end the developers have to agree on new proposed authentication mechanisms as well as being able to implement them and integrate them in existing services and tools. Therefore, we decided to study the different identified requirements further with an online survey with developers. The goal of the survey was, on the one hand, to confirm that the identified requirements were indeed relevant for developers. On the other hand, we wanted to determine whether the list of requirements should be extended in terms of additional aspects. Furthermore, it allowed us to test further types of requirements namely evidence and developer issues which were not mentioned in the authentication literature we reviewed for Section 3 but are often mentioned in literature in related areas.

We posted a link to an online survey on various developer forums. 93 developers responded to our survey, of whom 72% developed systems for the desktop, 2% developed for mobile environments only and the rest developed for both. We asked whether they had had any experience of authentication other than the password. 34% had had some experience of authentication other than the password although 73% were aware that alternatives to passwords existed. 60% said they were aware of situations where the password was not particularly suitable and 96% said they would consider using an alternative mechanism if it were shown to be better for a particular user group. We asked them what would convince them to switch to an alternative authentication mechanism. We offered them the following possible reasons based on the literature reviewed in Section 3. They could select as many options as they wanted.

(1) risk mitigation: strength wrt. guessability, observability, recordability;

(2) quality in use: easier for users to use and remember;

(3) business context: it would reduce costs (either for user, infrastructure or adminstration);

We did not specifically mention user context because we wanted to see whether the developers mentioned this themselves as aspects of user context are not that obvious and are not mentioned very often in literature. We included '**evidence: other companies have used it successfully**' although it has not mentioned in the context of authentication literature we reviewed for Section 3, in order to confirm the importance of *stories* in convincing organisations to use new technologies [14, 15]. We also included the option '**developer issues: easy to use API**'. This type of requirement was added as software engineering

researchers in general argue for the benefits of reusable components in software development (see e.g. [31]). We also offered them a text field to add their own reasons or thoughts, in order to get new types or aspects if there are any.

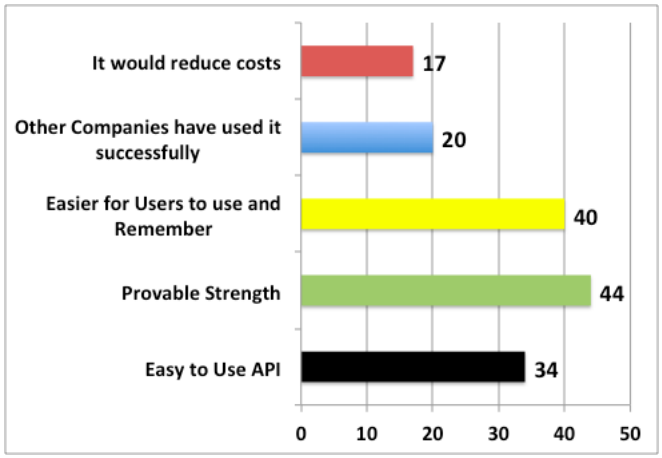

Fig. 3. Confirming Requirements

Figure 3 shows the result: User Context did indeed emerge from the developers' comments. In general, all comments could be assigned to at least one of the identified requirements. Sample comments are:

- *Risk Mitigation*: "It should resist observation attempts"
- *Quality in Use*: "Whether it was accessible to blind and deaf users", "Ease of authenticator replacement"
- *Business Context*: "It must hold value for the company and the end user", "It should not be too costly"
- *User Context*: "Whether it could be used on multiple platforms"
- *Evidence*: "Depends on how strong the evidence is", "Ease of implementation"

5 Integration of Requirements into ACCESS

The developer survey led to the decision to include 'evidence' and 'developer issues' in the ACCESS framework although it was not mentioned in the authentication literature. 'Developer issues' is included in *business context* and *evidence* is a different kind of element. Evidence encompasses 'risk mitigation', 'quality of use', 'business context', and 'user context' aspects. While decision makers can provide information about requirements in terms of risk, target end-users, business and user context, they might only be willing to trial schemes supported by hard evidence i.e. other organisations have used such a mechanism successfully or the evidence from the academic literature is very convincing.

In Figure 4, the above-mentioned type of requirements are incorporated into the ACCESS framework. While 'risk mitigation', 'quality of use', 'business context', and 'user context' are taken into account for the feasibility analyses and to describe the authentication alternatives in the knowledge base, existence of evidence is a property of schemes included in knowledge base and also added to the output. However, it is not taken into account for the feasibility analysis as only very few of the alternative authentication schemes have been deployed and tested in the wild. If ACCESS is successful this will change in future and then 'evidence' will become part of the feasibility analysis.

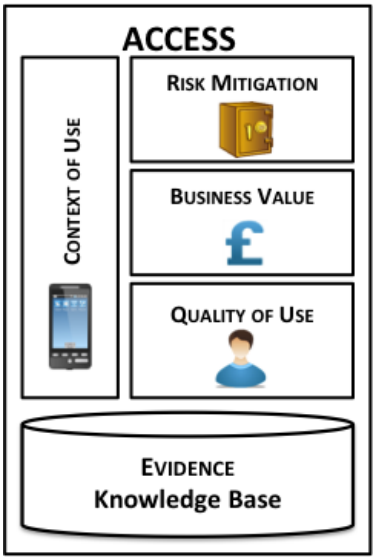

Fig. 4. Feasibility Factors Influencing Acceptance and Adoption of an Alternative Authentication Mechanism

In order to support this process and to iteratively extend the framework based on the results for piloting, it is essential for the framework facilitate simple and easy recording of pilot experiences. Such an interface should record the experiences in terms of the core requirements so that it can be matched to scenarios presented by subsequent framework users. If the framework is offered as a web-based decision-support system, this information can immediately be made available to other users. If it is offered as a stand-alone application, it should use a push mechanism to send this knowledge to a central repository for broadcast to other instances of the framework, as recommended by [32]. This will support independent and distributed augmentation of the knowledge repository with authentic and ecologically sound experiences from the field, creating a network of mutually reinforcing systems [33].

Note, although quality of use is considered in the feasibility analyses, it is necessary to run acceptance studies with the selected alternative afterwards. This is caused by missing evidence from similar settings and the fact that the user studies from literature considering to evaluate quality of use aspects are very limited with respect to having studied a representative group of the population and with respect to long term issues. All this can finally only be assessed in use, in the wild, over time. For example, consider the following requirement specification:

- *Risk mitigation*: Low risk: essentially a community website.

- *Quality of use*: Elderly community members, all literate, all with corrected to normal vision, all with reasonable hearing, but with dexterity challenges. Can use basic features on a computer. Convenience is not a concern for these

users.

- *Business context*: Small budget.

- *Context of use*: They will be using the mechanism from home and library computers, but not from smartphones, or on the move. The purpose of the authentication is to enforce accountability since members can post blog items. There is no current website, and usage is expected to be bi-weekly (fairly infrequent).

If we implement Korhonen *et al.*'s [20] first approach: eliciting requirements and generating a ranked list of alternatives, the ACCESS framework might feasibly generate the following ranking:

Musical Password [34]. This mechanism has been tested with a wide range of users, and was very favourably received by the elderly participants. It requires users to choose from a number of music clips, all of which feature 1960s music. At authentication users identify "their" clips. In terms of memorability it performed well across all user groups.

Recognition-Based Graphical Authentication [35]. This mechanism was designed specifically for a user group as depicted in the scenario depicted above. Users identify their own PIN, postal code and doodle from subsequent challenge sets composed of image grids. It has proved extremely popular and has been in use for 9 years now.

6 Conclusion

Alternative authentication technologies have not captured the minds and hearts of developers, users, and decision makers. However, the pressures on the (textual) password have increased to such an extent that it is necessary for decision makers to rethink this 'safe' strategy and start thinking of other ways of controlling access to their systems. We cannot realistically expect one alternative to replace the ubiquitous (textual) password, but we propose to use a wider variety of authentication mechanisms. To support decision makers to select appropriate once, trial them, and subsequently to adopt them, we propose the ACCESS framework. Future work will develop the the knowledge base and an interface which captures the decision's requirements and matches that to candidate authentication mechanisms to support informed choice.

References

1. A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.
2. S. Chiasson, R. Biddle, and P. C. van Oorschot, "A Second Look at the Usability of Click-Based Graphical Passwords," in *Proc. 3rd Symposium on Usable Privacy and Security*, 2007, pp. 1 – 12.

3. W. Moncur and G. Leplâtre, "Pictures at the ATM: Exploring the Usability of Multiple Graphical Passwords," in *Proc. SIGCHI Conference on Human Factors in Computing Systems (CHI'07)*, 2007, pp. 887 – 894.
4. E. Stobert, A. Forget, S. Chiasson, P. van Oorschot, and R. Biddle, "Exploring Usability Effects of Increasing Security in Click-Based Graphical Passwords," in *Proc. 26th Annual Computer Security Applications Conference (ACSAC '10)*, 2010, pp. 79 – 88.
5. R. W. Frischholz and U. Dieckmann, "BioID: A Multimodal Biometric Identification System," *IEEE Computer*, vol. 33, no. 2, pp. 64 – 68, 2000.
6. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14(1), January 2004, pp. 4–20.
7. M. Conti, I. Zachia-Zlatea, and B. Crispo, "Mind How You Answer Me! Transparently Authenticating the User of a Smartphone when Answering or Placing a Call," in *Proc. 6th ACM Symposium on Information, Computer, and Communications Security*, 2011, pp. 249 – 259.
8. A. D. Frankel and M. Maheswaran, "Feasibility of a Socially Aware Authentication Scheme," in *Proc. 6th IEEE Consumer Communications and Networking Conference*, 2009, pp. 1–6.
9. M. D. Corner and B. D. Noble, "Zero-interaction Authentication," in *Proc. 8th Annual International Conference on Mobile Computing and Networks*, 2002, pp. 1 – 11.
10. L. Catuogno and C. Galdi, "On the security of a two-factor authentication scheme," in *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*. Springer, 2010, pp. 245–252.
11. D. Recordon and D. Reed, "OpenID 2.0: a platform for user-centric identity management," in *Proceedings of the second ACM workshop on Digital identity management*. ACM, 2006, pp. 11–16.
12. K. Renaud, P. Mayer, M. Volkamer, and J. Maguire, "Are graphical authentication mechanisms as strong as passwords?" in *Frontiers in Network Applications, Network Systems and Web Services (SoFAST-WS'13)*, Kraków, Poland, September 8-11, 2013.
13. F. Schaub, M. Walch, B. Könings, and M. Weber, "Exploring the design space of graphical passwords on smartphones," in *Symposium on Usable Privacy and Security (SOUPS)*, Newcastle, UK, 24-26 July, 2013.
14. C. Heath and D. Heath, *Made to Stick: Why some ideas take hold and others come unstuck*. Arrow Books, 2008.
15. M. Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*. Abacus, 2001.
16. A. M. O'Connor, P. Tugwell, G. A. Wells, T. Elmslie, E. Jolly, G. Hollingworth, R. McPherson, H. Bunn, I. Graham, E. Drake *et al.*, "A decision aid for women considering hormone therapy after menopause: Decision support framework and evaluation," *Patient education and counseling*, vol. 33, no. 3, pp. 267–280, 1998.
17. J. Park and T. W. Simpson, "Development of a production cost estimation framework to support product family design," *International journal of production research*, vol. 43, no. 4, pp. 731–772, 2005.
18. J. Dong, H. S. Du, S. Wang, K. Chen, and X. Deng, "A framework of web-based decision support systems for portfolio selection with OLAP and PVM," *Decision Support Systems*, vol. 37, no. 3, pp. 367 – 376, 2004.

19. A. X. Garg, N. K. Adhikari, H. McDonald, M. P. Rosas-Arellano, P. Devereaux, J. Beyene, J. Sam, and R. B. Haynes, "Effects of computerized clinical decision support systems on practitioner performance and patient outcomes," *JAMA: the journal of the American Medical Association*, vol. 293, no. 10, pp. 1223–1238, 2005.
20. P. Korhonen, H. Moskowitz, and J. Wallenius, "Multiple criteria decision support. A review," *European Journal of Operational Research*, vol. 63, no. 3, pp. 361–375, 1992.
21. A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 128–152, 2005.
22. G. M. Beal, E. M. Rogers, and J. M. Bohlen, "Validity of the concept of stages in the adoption process," *Rural Sociology*, vol. 22, no. 2, pp. 166–168, 1957.
23. C. Herley, P. C. van Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?" in *Proc. Financial Cryptography 2009*, 2009.
24. Z. Mack and S. Sharples, "The importance of usability in product choice: A mobile phone case study," *Ergonomics*, vol. 52, no. 12, pp. 1514–1528, 2009.
25. E. J. Kelley, "The importance of convenience in consumer purchasing," *The Journal of Marketing*, pp. 32–38, 1958.
26. C. S. Weir, G. Douglas, M. Carruthers, and M. Jack, "User perceptions of security, convenience and usability for ebanking authentication tokens," *Computers & Security*, vol. 28, no. 1-2, pp. 47–62, 2009.
27. L. Tam, M. Glassman, and M. Vanderwauver, "The psychology of password managementl a tradeoff between security and convenience," *Behaviour & Information Technology*, vol. 29, no. 3, pp. 233–244, 2010.
28. L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.
29. A. Monk, "User-centred design," in *Home Informatics and Telematics*. Springer, 2000, pp. 181–190.
30. J. Maguire, "An ecologically valid evaluation of an observation-resilient graphical authentication mechanism," Ph.D. dissertation, Computing Science, 2013.
31. Y. Yang, J. Bhuta, B. Boehm, and D. N. Port, "Value-based processes for COTS-based applications," *Software, IEEE*, vol. 22, no. 4, pp. 54–62, 2005.
32. I. Sim, P. Gorman, R. A. Greenes, R. B. Haynes, B. Kaplan, H. Lehmann, and P. C. Tang, "Clinical decision support systems for the practice of evidence-based medicine," *Journal of the American Medical Informatics Association*, vol. 8, no. 6, pp. 527–534, 2001.
33. J. Ferguson, M. Bell, and M. Chalmers, "Mutually reinforcing systems," in *Proceedings of the ACM SIGKDD Workshop on Human Computation*, ser. HCOMP '10. New York, NY, USA: ACM, 2010, pp. 34–37.
34. M. Gibson, K. Renaud, M. Conrad, and C. Maple, "Musipass: Authenticating me softly with my song," in *Proceedings of the 2009 Workshop on New security paradigms workshop*. ACM, 2009, pp. 85–100.
35. K. Renaud and J. Ramsay, "Now what was that password again? A more flexible way of identifying and authenticating our seniors," *Behaviour & Information Technology*, vol. 26, no. 4, pp. 309–322, 2007.