5th ISCA/DEGA Workshop on Perceptual Quality of Systems (PQS 2016)
29-31 August 2016, Berlin, Germany

User Experience in Authentication Research: A Survey

Lydia Kraus, Jan-Niklas Antons, Felix Kaiser, Sebastian Möller

Quality and Usability Lab, Telekom Innovation Laboratories, TU Berlin, Germany
{lydia.kraus, jan-niklas.antons, felix.kaiser, sebastian.moeller}@telekom.de

Abstract

We present a structured literature survey of User Experience (UX) dimensions and influencing factors in authentication research. The survey is based on authentication papers presented between 2010 and 2015 on the major human-computer interaction (HCI) and usable privacy and security (UPS) venues. 19% of the found papers include UX topics. Those papers show that there is a variety of ways how authentication research can profit from UX. Nevertheless, UX is often rather a by-product and not recognized as a field of study. We further discuss opportunities and challenges of including UX in authentication research.

Index Terms: user experience, usable security and privacy, authentication, survey

1. Introduction

Around the year 2000, a new field of study emerged in the human-computer interaction (HCI) research community. Whereas until this time, the focus of determining system qualities has been rather on instrumental and functional aspects such as usability and successful task completion, researchers got more and more interested in viewing interactions with products in a broader context [1]. This broad view on user interactions with systems and products - conceptualized in the term *user experience (UX)* - focuses on users' experiences with a product or system, for instance in terms of affect and emotion, non-instrumental product qualities, and situatedness of interaction [2].

At the same time, starting around 1995 the research field of usable privacy and security (UPS) emerged [3]. Thereby, researchers began to promote the idea of stimulating 'security-supportive' user behavior and adoption of security and privacy systems by improved usability and user-centered design [3]. However, usability and security or privacy have since then often been found to be conflicting, as reducing system complexity to achieve usability might result in reduced security or privacy.

As the name indicates, UPS is mainly concerned with making privacy and security systems more usable. Nevertheless, UPS can profit from lessons learned from the field of UX: UX can help to gather a rich understanding of users' practices and of usage situations, thus leading to new insights on the design of security systems beyond usability [4].

So far, there is little known about the opportunities and challenges that result from including UX in UPS research. Therefore, we conducted a structured literature review to gain insights on how UX topics have been taken up in UPS research. We take the topic of authentication as a canonical example to study our research question as authentication is one of the major topics in UPS research and has been intensively studied in the literature [3]. We investigate which UX dimensions and influencing factors are addressed in works on authentication, how methods to evoke UX can support the design of new authentication mechanisms, and which challenges might result thereof.

We identify several opportunities of including UX into authentication research: for example, UX-based approaches can serve as a design inspiration for authentication mechanisms and they help in understanding users' practices around using authentication mechanisms, and their impact on security. We furthermore discuss possible challenges resulting from including UX-based approaches in authentication mechanism design. Despite the given opportunities, we find that UX in authentication research is often rather a by-product and not recognized as a field of study.

2. Related work

In order to analyze aspects of UX in authentication research, we will first define our notion of the UX concept, its dimensions, and its influencing factors. Thereafter, we give a brief introduction to authentication research topics and related security and usability issues.

2.1. User experience: Dimensions and Influencing Factors

UX can be seen as a phenomenon, as a field of study, and as a practice [5]. Our notion of UX mainly refers to the second definition, i.e. a field of study. We understand UX as a multi-faceted construct which consists of several dimensions. Furthermore, there are a number of factors which may influence a user's experience with a system. We refer to those as "influencing factors". In the following, common UX dimensions and influencing factors which are described in fundamental UX works and in prior UX survey papers are discussed [6, 7, 8, 2, 1, 9].

A goal of UX research is to gain a **rich understanding** of users' experiences with the object of study [6, 7, 1]. This understanding can be either gained by using open-ended study methods (such as open-ended interviews or questionnaires) or by referring to different dimensions of UX: For example, **affect**, **emotion**, and **feelings** have been found to be important dimensions of UX [2, 6, 1]. Other UX dimensions are **non-instrumental product qualities** such as hedonic quality, aesthetics, and beauty [2, 1]. UX can also encompass the dimension of user **motivation** [1] and include **social factors** [2]. **Engagement and flow** are further dimensions of user experience which have, however, only received minor attention in studies of UX [1].

Furthermore, there are factors that influence how an experience is perceived by the user: UX may change depending on the **context** and is thus situated [7, 2, 9, 1, 6]. UX is moreover considered to be **dynamic** and **time dependent** [2, 9, 6, 1]: it may change over time and is not constant. The last topic which is considered in this paper are the **methods** that can be used to evoke an experience. Those include for instance providing users with meaningful or stimulating interactions, or with systems

10.21437/PQS.2016-12

that offer the opportunity to identify themselves with [6, 8]. We consider user experience as something more than usability, thus usability in terms of performance measures (such as efficiency and effectiveness) is not considered as an element of UX in this paper.

2.2. Background: Authentication

The scope of this paper is authentication of users towards a system. In an authentication process, a user typically identifies herself with a User ID and it is then verified whether she is the "legitimate owner of this ID" [10]. There are three main areas of authentication: knowlegde-based, token-based, and biometric authentication. The verification process of knowledge-based authentication relies on something the user knows, i.e. the password. The essence of designing a secure system is the deployment of a threat model. The resulting challenge for evaluating such systems in user studies is to correctly deploy the threat model and to test the system in the light of attacks [3]. Knowledge-based authentication systems face two kind of threats, namely those arising from password guessing attacks and those arising from password capturing attacks [11]. Thereby, the user has a non-negligible influence on the security of the system when selecting a password. There is a trade-off between usability and security in authentication. For instance, random passwords are more secure compared to user-selected passwords, but they are harder to remember [12]. User behavior often reflects this trade-off and may create as a consequence security vulnerabilities: For example, if a weak password is chosen by the user, the authentication system may be more vulnerable to guessing attacks. Also, to easier remember passwords, user may write them down. However, this might lead to the situation that those "documented" passwords are easy to capture by adversaries. Therefore, common challenges in knowledge-based authentication encompass the usability and security of passwords (e.g. textual, alphanumerical, or graphical) and password managers [3].

Token-based authentication relies on something a user has, e.g. a device or hardware token [3]. An example of a token-based authentication process is the withdrawal of money from an ATM. Thereby, the authentication process is built upon two factors: token (the card) and knowledge (the PIN). A vulnerability of token-based systems is that the token may be stolen by an attacker.

The third class of authentication systems, biometric systems, seem on the first glance to overcome the limitations of knowledge-based authentication. Biometric verification relies on "anatomical, physiological or behavioral" information of a user [13, 3]. Examples for biometric authentication methods include fingerprint recognition or gesture recognition. Biometric authentication does not possess the vulnerabilities of knowledge-based authentication such as weak password choices and password documentation. Nevertheless, there are limitations of biometric authentication as anatomical, physiological, and behavioral information can be spoofed. For example, fingerprints can be easily collected - even remotely - with a high-resolution camera on a smartphone during the usage of the smartphone [14]. For biometric authentication, accuracy and performance of biometric systems as well as vulnerabilities of such systems are popular research topics [3].

3. Methodology

We used the UX dimensions and influencing factors defined in Section 2 to survey papers from three major conferences: The ACM SIGCHI Conference (CHI) as it is the main venue in the field of HCI and a popular publication venue for UPS researchers [3], the Symposium on Usable Privacy and Security (SOUPS) – the "only stand-alone conference devoted solely to the publishing of usable privacy and security research" [3, p. 20], and the main venue for HCI research in the mobile context - the International Conference on Human-Computer Interaction with Mobile Devices and Services (mobileHCI). The latter venue was included due to the fact that UX research often happens in the context of mobile applications and services [1].

We considered full and short papers, posters, and workshop papers published between 2010 and 2015 on those venues. Papers considered as "authentication papers" had to either contain one of the predefined search terms (authentication, password, access and access control, lock) in their title or had to be presented in a session that had one of the search terms in its title.

We extracted 180 papers in total. After removing duplicates (e.g. papers that have been published as a poster before), 167 papers remained. Those papers were then screened by titel and abstract by the first author to determine whether they explicitely or implicitely contain UX topics. Besides including UX topics, papers to be included in the survey had to further fulfill the following criteria: to be about authentication in the sense that a user authenticates herself towards a system, *not* to solely focus on security assessments, *not* to solely focus on usability performance measures, *not* to solely focus on study methods, and *not* to solely focus on the economics of security. 20% of the 167 papers (34 papers) were screened by one of the other authors who also made a decision which of them to include. This action served to control for the reliability of the procedure and is based on [1]. Interrater agreement on which papers to include was found to be substantial (Cohen's $\kappa = 0.68$, $p < 0.001$). Finally, 32 papers (19%) remained for detailed analysis[1]. Those papers were analyzed in detail by two of the authors regarding the UX topics they contain, the study methods they use, and the authentication topics they cover.

4. Results

As can be seen in Table 1, papers, which were analyzed in detail, revealed that gaining a rich understanding was the most often addressed point (50%), followed by methods to evoke UX (31%), and the UX dimensions of affect, emotion, and feelings (22%) as well as motivation (22%). A number of papers addressed influencing factors of UX such as situatedness and context (16%) and social factors (9%). An assessment of user behavior over time was done in one paper (3%). Note, that we did not consider repeated measurements of performance (system performance or password memorability) as describing dynamic and time-dependent UX. Interestingly, none of the papers dealt with non-instrumental product qualities of authentication systems (e.g. hedonic quality) or with flow and engagement during authentication.

All included papers contained UX topics; however, UX is seemingly in many of the works not recognized as a field of study: only seven (22%) of the analyzed papers explicitely re-

[1]Please refer to the following link for the list of analyzed papers: `http://www.redaktion.tu-berlin.de/fileadmin/fg41/users/kraus-lydia/PQS2016_UX_Security_Literature_List.pdf`

Table 1: UX topics addressed in papers on authentication. Papers can contain multiple topics.

UX topics in authentication research	# of papers	%
Rich understanding	16	50%
Methods to evoke UX	10	31%
Affect, emotion, feelings	7	22%
Motivation	7	22%
Situatedness, context	5	16%
Social factors	3	9%
Time-dependency, dynamic	1	3%
Non-instrumental product qualities	0	0%
Engagement, flow	0	0%

ferred to the terms "user experience" or "experience" in their abstract or title. Twenty-five (78%) of the analyzed papers, however, contained the term "experience" at least once in their body.

In the following, we detail how UX topics were addressed in authentication papers regarding "rich understanding", "methods to evoke UX", and "affect, emotion, and feelings". Due to space constraints, we limit the details to the three top-most topics of Table 1. Moreover, the fourth dimension - Motivation - is also represented in most of those topics, as we allowed papers to be assigned to multiple topics. For each topic, we also provide a summary of 1-3 papers which are in our opinion representative for this topic.

4.1. Gaining a rich understanding of (knowledge-based) authentication

A high amount of the analyzed papers (50%) aim at a better understanding of users' experiences and interactions with authentication systems. We identified knowledge-based authentication as the major topic in the category of "rich understanding" with two major sub-categories: users' password handling practices and the interaction with mobile authentication systems.

Papers on users' password handling practices include the investigation and exploration of a variety of issues such as users' coping strategies for managing a high number of passwords (e.g. [15]), users' strategies for password creation (e.g. [16]), password use in the wild and in daily life (e.g. [17, 18]), password policy handling (e.g. [19]), and password sharing between users (e.g. [20]).

The paper by Dunphy et al. [21] constitutes an illustrative example of how self-reported user experiences can enable researchers to gain broad insights into complex password handling practices: in their paper they analyze user experiences that were collected through tweets on the micro-blogging site Twitter. Thereby they find for example that passwords can serve as "social currency" with which people define relationships and their degree of closeness to others [21]. This provides a new view point on password management behavior and encourages the notion that authentication is more to users than the trade-off between usability and security.

The papers from the second sub-category, i.e. mobile authentication, are concerned with the investigation of smartphone locking in daily life and in real life settings (e.g. [22]). An example here is the paper by Harbach et al. [23] in which the experience sampling method is used to investigate locking and unlocking actions on smartphones. They find that non-users felt that authentication is not necessarily needed to feel that their smartphone is protected [23]. This provides insights on non-users and their motives - knowledge that might inspire new ways of authentication targeting current non-users' needs.

Regarding the study methods, qualitative and mixed methods approaches were the dominating study methods in the "rich understanding" category: half of the papers in this category used qualitative approaches such as interviews or open-ended questionnaires, whereas approximately the other half (44%) used mixed method approaches (qualitative and quantitative approaches).

The papers in the "rich understanding" category encompass a variety of topics and provide rich empirical data upon which future work can build.

4.2. Methods to evoke UX as inspiration for authentication systems

All papers in the "methods" category present new authentication systems or prototypes thereof. Those papers can be further divided into two sub-categories: papers in the first subcategory target usability and/or security issues in the design of authentication systems such as improving the memorability of passwords, supporting the creation of secure passwords, and reducing the effort for authentication. Methods which are known from UX research as facilitator of user experience are more or less "unintentionally" deployed in these systems. This means that it is not explicitely stated that the methods are related to UX, but they are interpreted by us as such. Examples of the papers in the first sub-category are those by Woo et al. [24] and Hang et al. [25]: password creation may be supported by asking users to assemble passwords from meaningful life experiences [24] or fallback authentication may use security questions about locations which are related to meaningful experiences (such as the location of "one's longest travel so far") [25].

These methods implicitely rely on "evocation". In the context of UX, Hassenzahl [8] defines evocation as the ability of a product to "provoke memories". Thereby, evocation is one of three characteristics (besides Stimulation and Identity) which may make a user perceive a product as offering hedonic qualities, i.e. provide the user with aspects of user experience that are more than the purely functional [8]. Unfortunately, so far, we were not able to find data on the user experience the described authentication systems [24, 25] offer in terms of different UX topics as defined in Section 2.

In terms of security, authentication methods that rely on meaningful experiences may suffer from vulnerabilities. For instance, when including personal experiences into knowledge-based authentication, it needs to be considered that this knowledge might be also known to "attackers" from a users' social circle. The location-based questions suggested by Hang et al. [25] which are related to meaningful events promise a good potential to be easy to answer and recall by a legitimate user and hard to guess by an attacker according to their study results.

An example of authentication methods that use the UX dimensions of motivation for improved password creation is the work by Eargle et al. [26]: they describe the deployment of different motivational statements for feedback in password meters. Thereby, the motivational statements are built on different methods such as scaring the users (by emphasizing threats) or teasing the users (by using humorous statements) in order to make them create more secure passwords. However, while the motivational statements seem to impact the password choice and were perceived as helpful by the users [26], again, we were not able to find data to which degree the motivational statements impact

the password security and whether they have an influence on the UX beyond functional aspects such as helpfulness.

While papers in the first sub-category of the "methods" UX dimension aim to improve usability and security by the help of UX methods, papers in the second sub-category explicitely target positive UX as a design goal of authentication systems. Examples of papers in the second sub-category are those by Karlesky et al. [27, 28]. As a method to evoke a positive experience Karlesky et al. use full-body gestures as the literature suggests body movement to be related to emotions [28]. In a prototype of an access control system, full body gestures are at the same time used to evoke pleasurable and playful interactions and as a mean for authentication [28]. The prototype of the described access control system was tested in an wizzard-of-oz experiment [28]. This makes it difficult to derive conclusions on the security and feasability of such a system.

The above mentioned examples indicate that researchers start to deploy methods grounded in UX research to improve the usability of, security of, and user experience with authentication systems. New threats may arise with such methods and have thus to be carefully considered during the design of new authentication systems.

4.3. Affect, emotions, and feelings related to authentication

Papers investigating affective, emotional and felt experience dimensions of authentication were found to be related to biometric authentication and to knowledge-based authentication in terms of password creation.

Regarding biometric authentication systems, De Luca et al. [29] find that (besides good usability) also positive emotional outcomes such as fun and joy play an important role as motivators for the adoption of fingerprint-based authentication on smartphones. They further find that negative emotional outcomes such as annoyance may lead to the abandonment of face-recognition-based authentication on smartphones [29]. Aumi and Kratz [30] find for gesture-based authentication that security and user experience do not necessarily need to contradict each other. Their authentication system, which is based on gesture-based authentication, has (in a lab study) shown to be able to evoke positive emotions during interaction even for complicated, i.e. more secure, gestures [30].

Regarding knowledge-based authentication, researchers showed to be interested in the feelings during password creation such as comfort [31] and sentiment in terms of annoynce and difficulty [32].

Most of the papers in this category deployed self-developed questionnaires to measure affect, emotions, and feelings. Standardized approaches for measuring affect and emotion were deployed in three papers: two of the seven papers in this category used the EmoCard technique [33], and one paper deployed the Self-assessment Manikin (SAM) [34] and the Affect Grid [35]. Furthermore, the paper by Haque et al. [31] presents the development of a questionnaire to measure comfort during password creation.

The outcomes of the papers in this category indicate that it is worthwhile to consider the emotional dimension in the evaluation of authentication systems.

5. Discussion and Conclusion

In the following we discuss the implications of our findings in terms of opportunities and challenges for UX in authentication research.

5.1. Limitations

Our paper is a first step towards identifying the topics, opportunities and challenges that UX in authentication research offers. Therefore, we limited the literature survey to three venues and a time frame of 6 years. There may be also other papers (not considered in the survey) which would provide interesting insights on the topic. Nevertheless, we suspect that the selected venues represent well the topics and methods of concurrent authentication research with a focus on human factors.

5.2. Opportunities of User Experience in Authentication Research

The results of the survey indicate that little work is conducted to investigate the potential of authentication systems to provide users with non-instrumental product qualities, such as hedonic quality. An opportunity for future authentication research is to investigate whether it is possible to address such aspects in authentication systems, and whether adressing such aspects can yield to increased adoption of authentication systems or supporting "security-supportive" behavior.

The development of user behavior over time was only adressed in one paper. Thus, there is a research gap on how user experience with authentication changes over time. Considering the temporal development of user experience might provide an explanation for negative changes in user behavior such as abandoned usage.

The results further indicate that the use and adoption of biometrics seems to be influenced by positive and negative emotions and feelings. How positive emotions can be systematically addressed in authentication systems is an interesting research question for future works. Another interesting research question is whether positive feelings during authentication can also impact security behavior in a positive way.

Papers employing methods to evoke UX show how UX can serve as a design inspiration to improve the usability of, the security of, and the user experience with authentication methods. Systematically identifying UX methods appropriate for the design of authentication systems is an opportunity for future research.

5.3. Challenges of User Experience in Authentication Research

The fact that a large number of the analyzed papers did not refer to user experience in their abstracts and titles suggests that while the concept of UX seems to be valuable for UPS research, further awareness raising from UX as a field of study and conceptualizations for the deployment of UX dimensions in UPS research are needed. Thereby, the integration of UX into existing and new threat models is another important aspect.

Our results indicate that for papers deploying UX methods to improve usability and security of authentication, little is known about how these approaches affect the user experience according to the different dimensions defined in Section 2. By contrast, papers that deploy UX methods to improve user experience seem to lack data on the system performance in terms of security. This suggests that more work is needed to investigate user experience with authentication systems, as well as threat models and the security impact of authentication systems that deploy methods which are grounded in UX.

6. References

[1] J. A. Bargas-Avila and K. Hornbæk, "Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2689–2698.

[2] M. Hassenzahl and N. Tractinsky, "User experience-a research agenda," *Behaviour & information technology*, vol. 25, no. 2, pp. 91–97, 2006.

[3] S. Garfinkel and H. R. Lipford, "Usable security: History, themes, and challenges," *Synthesis Lectures on Information Security, Privacy, and Trust*, vol. 5, no. 2, pp. 1–124, 2014.

[4] P. Dunphy, J. Vines, L. Coles-Kemp, R. Clarke, V. Vlachokyriakos, P. Wright, J. McCarthy, and P. Olivier, "Understanding the Experience-Centeredness of Privacy and Security Technologies," in *Proceedings of the 2014 workshop on New Security Paradigms Workshop*, 2014, pp. 83–94.

[5] V. Roto, E. Law, A. Vermeeren, and J. Hoonhout, "User experience white paper," *Bringing clarity to the concept of user experience*, 2011.

[6] J. McCarthy and P. Wright, "Technology as experience," *interactions*, vol. 11, no. 5, pp. 42–43, 2004.

[7] M. Hassenzahl, "Experience design: Technology for all the right reasons," *Synthesis Lectures on Human-Centered Informatics*, vol. 3, no. 1, pp. 1–95, 2010.

[8] ——, "The thing and i: understanding the relationship between user and product," in *Funology*. Springer, 2003, pp. 31–42.

[9] E. L.-C. Law, V. Roto, M. Hassenzahl, A. P. Vermeeren, and J. Kort, "Understanding, scoping and defining user experience: a survey approach," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2009, pp. 719–728.

[10] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[11] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[12] J. Yan *et al.*, "Password memorability and security: Empirical results," *IEEE Security & privacy*, no. 5, pp. 25–31, 2004.

[13] L. Coventry, "Usable biometrics," in *Usable Security - Designing Secure Systems that People Can Use.*, L. Cranor and S. Garfinkel, Eds. Cambridge, MA: O'Reilly, 2005, pp. 175–198.

[14] T. Fiebig, J. Krissler, and R. Hänsch, "Security impact of high resolution smartphone cameras," in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, 2014.

[15] E. Stobert, "The agony of passwords: can we learn from user coping strategies?" in *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2014, pp. 975–980.

[16] B. Ur, F. Noma, J. Bees, S. M. Segreti, R. Shay, L. Bauer, N. Christin, and L. F. Cranor, ""' i added'!'at the end to make it secure": Observing password creation in the lab," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 123–140.

[17] P. Inglesant and M. A. Sasse, "Studying password use in the wild: practical problems and possible solutions," in *SOUPS 2010: Workshop on Usable Security Experiment Reports*, 2010.

[18] E. Hayashi and J. Hong, "A diary study of password usage in daily life," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2627–2630.

[19] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2010, pp. 383–392.

[20] J. Kaye, "Self-reported password sharing strategies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2619–2622.

[21] P. Dunphy, V. Vlachokyriakos, A. Thieme, J. Nicholso, J. McCarthy, and P. Olivier, "Social media as a resource of security experiences: A qualitative analysis of #password tweets," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 123–140.

[22] E. Von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. ACM, 2013, pp. 261–270.

[23] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "Itsa hard lock life: A field study of smartphone (un) locking behavior and risk perception," in *Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 213–230.

[24] S. S. Woo, J. Mirkovic, and E. Kaiser, "Life-experience passwords (leps)," in *Who are you?! Adventures in Authentication: WAY Workshop; SOUPS*, 2014.

[25] A. Hang, A. De Luca, M. Smith, M. Richter, and H. Hussmann, "Where have you been? using location-based security questions for fallback authentication," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 169–183.

[26] D. Eargle, J. Godfrey, H. Miao, S. Stevenson, R. Shay, B. Ur, and L. Cranor, "Poster: You can do better–motivational statements in password-meter feedback," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015.

[27] M. Karlesky, N. Sae-Bae, K. Isbister, and N. Memon, "Who you are by way of what you are: Behavioral biometric approaches to authentication," in *Who are you?! Adventures in Authentication: WAY Workshop; SOUPS*, 2014.

[28] M. Karlesky, E. Melcer, and K. Isbister, "Open sesame: reenvisioning the design of a gesture-based access control system," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2013, pp. 1167–1172.

[29] A. De Luca, A. Hang, E. von Zezschwitz, and H. Hussmann, "I feel like i'm taking selfies all day!: Towards understanding biometric authentication on smartphones," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 1411–1414.

[30] M. T. I. Aumi and S. Kratz, "Airauth: evaluating in-air hand gestures for authentication," in *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, 2014, pp. 309–318.

[31] S. T. Haque, S. Scielzo, and M. Wright, "Applying psychometrics to measure user comfort when constructing a strong password," in *Symposium On Usable Privacy and Security (SOUPS 2014)*, 2014, pp. 231–242.

[32] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2011, pp. 2595–2604.

[33] P. Desmet, K. Overbeeke, and S. Tax, "Designing products with added emotional value: Development and appllcation of an approach for research through design," *The design journal*, vol. 4, no. 1, pp. 32–47, 2001.

[34] J. D. Morris, "Observations: Sam: the self-assessment manikin; an efficient cross-cultural measurement of emotional response," *Journal of advertising research*, vol. 35, no. 6, pp. 63–68, 1995.

[35] J. A. Russell, A. Weiss, and G. A. Mendelsohn, "Affect grid: a single-item scale of pleasure and arousal." *Journal of personality and social psychology*, vol. 57, no. 3, p. 493, 1989.