Exploring the Meaning of "Usable Security"

Markus Lennartsson, Joakim Kävrestad, Marcus Nohlberg

Exploring the meaning of "usable security"

Markus Lennartsson[1], Joakim Kävrestad[1], and Marcus Nohlberg[1]

University of Skövde, Sweden *firstname.lastname*@his.se

Abstract. While there are many examples of incidents that make the need for more work around the human aspects of security apparent, the literature makes it obvious that usable security can mean many different things and usable security is a complex matter. This paper reports on a structured literature review that analyzed what the research community considers to be included in the term "usable security". Publications from the past five years were analyzed and different perceptions of usable security were gathered. The result is a listing of the different aspects that are discussed under the term "usable security" and can be used as a reference for future research of practitioners who are developing security functions with usability in mind.

Keywords: Information Security · Usable · Usability.

1 Introduction

A lot of attention is currently given to the human, or user, side of information security and it is widely acknowledged that user behavior is a crucial factor in information security [74]. An important topic in this area is usable security, the notion that security tools and measures have to live up to usability demands in order to function as intended[73]. Tools that are lacking in usability are likely to not be used at all or be used incorrectly. If a given tool is not used, the security value that it is supposed to add will be lost. A tool that is used incorrectly can give a false sense of security, or even have a negative impact on security[81].

While there are many papers that provide usability evaluations on various tools and techniques, there is an ambiguity in the research community as to what the concept of usable security actually encompasses. There are several examples of papers that discuss or validate usability and two examples are [79] that evaluates certain usability criteria of a phishing defense mechanism and another is [75] where usability in access control in IoT is discussed. While valuable pieces of research, none of them discuss usability in a broader sense. Further, [77] evaluates usability around the keywords "convenience, annoyance, time-consuming and tiring" and builds on the System Usability Scale (SUS) presented by [72]. While the SUS scale measures important aspects of usability, it does not factor in ideas that [81] consider essential in usable security, for instance, that users should not make dangerous errors.

The existing research demonstrates that usable security is a complex area with many dimensions. However, to the best of our knowledge, there is no common definition or understanding of what the term actually includes. The aim of

this paper is to address this gap by reviewing how the term is applied in recent research. The result will describe what researchers mean with usable security and can be used as a reference for future studies. Future research will build on this paper with the goal of establishing evaluation criteria for usability is security tools and measures designed to be used by end-users.

2 Methodology

The research was carried out using a structured literature review targeting research published in the past five years. The review followed the process described by [78]. The outcomes of a literature review are heavily dependent on the databases used, search terms are chosen, and the criteria applied to select relevant literature [80, 76]. The databases and search terms used in this study are shown in Table 1, below.

Databases	Search Terms
ACM Digital library IEEExplore Springer Link dblp (Digital Bibliography & Library Project)	"usable security"
ArXiv SCOPUS CSCAN HAISA	usability AND security

Table 1. List of used databases and search terms

The initial searches resulted in 378 articles, papers that were duplicates or failed to meet inclusion criteria were removed resulting in 49 papers that were selected for further analysis. Backward snowballing, as described by [82], was employed and resulted in another 21 papers, resulting in 70 papers that were included for the study. Table 2 presents the inclusion and exclusion criteria used in this study and Table 3 shows the result of the initial selection process. Table 4 shows the results of the backward snowballing.

Inclusion criteria	Exclusion criteria
IC1: Published between 2015 and 2020	EC1: Publication occurs multiple times
IC2: Published in peer-reviewed journal or conference	EC2: Fails to meet inclusion criteria
IC3: Publication is relevant to the topic	EC3: Payment required for access
IC4: Written in English, Swedish or German	EC4: Dubious description of method or results

Table 2. Inclusion and exclusion criteria

Resource	Search date	Hits	Eliminated due to:				Accepted
			EC1	EC2	EC3	EC4	
ACM Dig. Lib.	20200102	12	145	159	15	10	49
IEEExplore	20200102	68					
Springer Link	20200102	14					
dblp	20200102	142					
ArXiv	20200102	20					
SCOPUS	20200111	102					
CSCAN HAISA	20200103	20					

Table 3. Initial search process

Resource	Search date	Hits	Eliminated due to:							Accepted
			IC1	IC2	IC3	IC4	EC1	EC3	EC4	
References in publications from stage I	20200116	1641	1250	161	147	57	1	3	1	21

Table 4. Snowballing process

The selected papers were analysed, using the software MAXQDA, using thematic coding as described by [71].

3 Results

Following the selection process, the included papers were analyzed using thematic coding. First, high-level aspects of usable security were identified. They were then refined into subcategories. The results are summarized in Figure 1, below, where the high-level aspects and their subcategories are displayed. The number in parenthesis shows the number of papers connected to a given subcategory.

The remainder of this chapter will describe the discovered aspects of usable security. The papers classified in each aspect will be referenced continuously and are listed in the reference list, preceded by an asterisk (*).

Cost of Use: This aspect addresses factors that users tend to perceive as inconvenient in terms of cost-effectiveness. *Financial* costs are mentioned repeatedly[1, 34, 25] and one publication [1] states that *resource consumption* (e. g. battery) might be of significance.

Consistency: Security solutions are perceived as usable when they are operating predictably. This applies to matters of *behavior* [34, 31], meaning that similar tasks work identically, and *implementation*[6, 55, 57] factors including standardized setups, consistent phrasing, and design that allows to easily recognize requirements and conditions.

Perception: Willingness to adopt security solutions depends partially on how they are perceived by individuals. One aspect relates to *trust and reputation*[61, 12, 10, 67, 11, 45, 25, 4, 36, 60]. Multiple studies report that users prefer

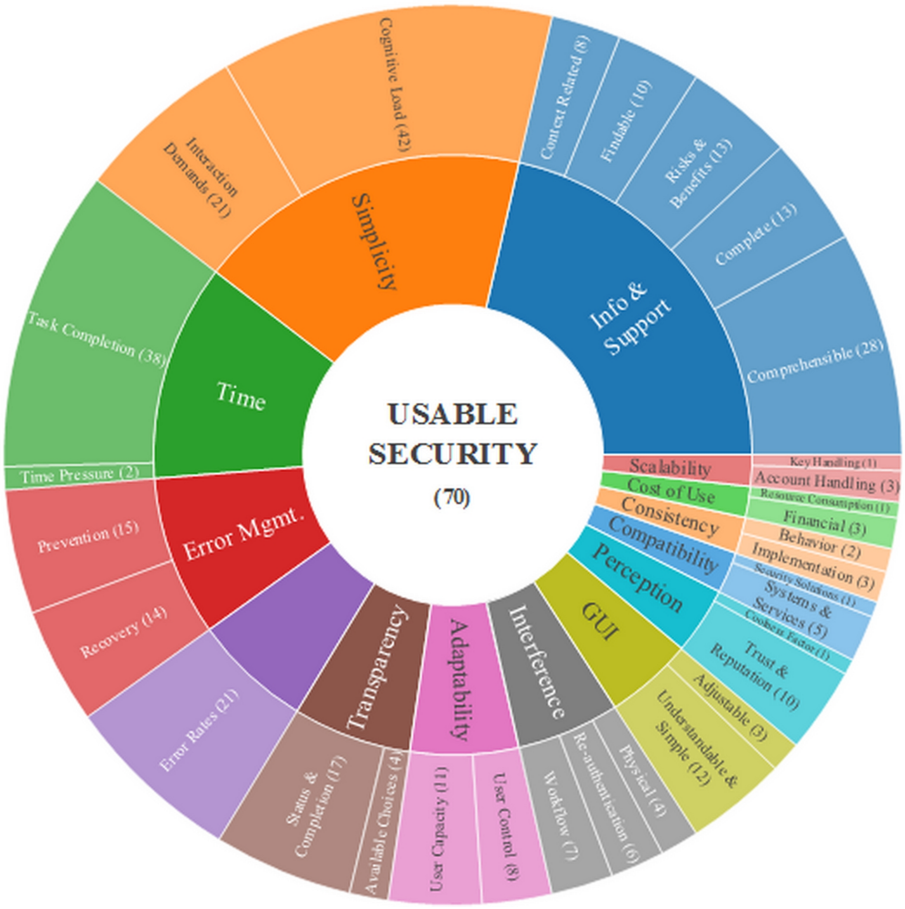

Fig. 1. Identified aspects of Usable Security. The number in parenthesis display the number of publications relation to each sub-category.

solutions they feel confident with. Such beliefs arise when a solution is from reputable sources, verified by experts, or recommended. Additionally, the *coolness factor* [61] of authentication schemes might be another contributing aspect.

GUI (Graphical User Interface): This aspect is concerned with the way the GUI is constructed. First, it should be *understandable and simple*[59, 69, 34, 51, 5, 40, 48, 49, 54, 55, 57, 66]. This includes visualization of navigation options and clear menu arrangements in accordance to what users might anticipate. Also, the GUI should not require unnecessary user attention and merely display information necessary for decision making. A GUI that is *adjustable* [6, 31, 55] to the user's preferences increases usability since it improves learnability.

Scalability: Another factor is the extent to which security solutions can deal with multiple user accounts and security keys. Usable *account handling*[22, 24,

57] does not restrict the number of allowed user accounts and allows to operate multiple accounts with mutual keys. Concerning *key handling* [12], a scalable solution should be able to install and control multiple keys without complicating usage.

Compatibility: Security solutions should be compatible with commonly used *systems and services*[20, 1, 22, 24, 57] to be perceived as usable. The trend of developing new security solutions with separate and fragmented user bases is a hinder to usability. Compatibility with other *security solutions* [1] is crucial since users will presumably reject overly incompatible products such as communication tools that only allow conversations with other instances of themselves.

Adaptability: How well a security solution can be adapted to the specific needs of individuals represents an important factor according to 19 publications. The first subcategory deal with the amount of allowed *user control*[20, 69, 22, 28, 31, 40, 49, 55]. Enabling users to customize configurations to their preferences increases convenience. Facilitating memorability by allowing users to choose their own passwords is also advantageous. Regarding *user capacity*[34, 51, 5, 12, 18, 27, 28, 38, 49, 55, 70], security solutions should be adaptable to various expertise levels and be able to, preferably intelligently, adapt to individual abilities and disabilities.

Interference: Usability is reduced when users' primary tasks are disturbed. The first subcategory addresses *workflow* [20, 63, 26, 27, 30, 49, 53] interference. Necessary security actions should be arranged in ways that minimize interruptions. Even *re-authentication*[3, 6, 14, 24, 27, 39] requests are described as disruptive and inconvenient . They can be perceived as wasted time and cause increased complexity. Also, compelling users to remember passwords repeatedly interrupts other tasks since enforced context switches may cause confusion. Finally, there is a *physical*[61, 15, 56, 57] category to this aspect. Users are anxious to lack immediate access to a token when needed, fear of loss or theft are common.

Error rate[20, 34, 63, 37, 3, 4, 17, 21, 26, 33, 35, 36, 38–40, 53, 57, 58, 66, 68, 70] To which extent a security solution enables users to conduct their primary task without having to deal with annoying completion failures is a prominent usability precondition. Increasing error rates cause substantial inconvenience since users are forced to repeat actions. Solutions become ineffective since they are unable to complete tasks as intended. In this context, it is secondary if errors are caused directly by the system or indirectly via users. When security solutions are error-prone, users may choose to circumvent them to preserve usability.

Error management: Effective means of *prevention*[59, 20, 69, 34, 67, 4, 6, 28, 31, 33, 48, 49, 54, 55, 57] are required to reduce error rates. Users should be provided with clear and simple instructions that help to prevent frequent errors. Incorrect operations can be prevented by automatic means such as input validity checks. Before errors occur, easy-to-understand warning messages should be communicated clearly and point out problem causes. Making users aware of their actions' negative consequences beforehand is beneficial. If such hints go unheeded, execution should be rejected. If errors cannot be prevented, proper means of error *recovery*[20, 34, 22, 4, 8, 12, 14, 29, 40, 49, 40, 54, 55, 57] should exist

to maintain usability. One way to recover is to allow users to cancel or revert their actions. Laborious recovery procedures are harmful to usability. Giving simple hints about causes and recommended actions are preferable. Users should be empowered to address most errors without external help, but help should still be available if needed.

Simplicity: A great quantity of studies report that users become overwhelmed by overly complex systems. Lots of papers stress that the *cognitive load* [44, 42, 34, 15, 10, 67, 11, 63, 45, 22, 51, 3, 2, 5–7, 9, 12–14, 19, 21, 24, 26, 28, 30, 30, 33, 36, 39–41, 49, 52–55, 57, 60, 62, 64, 66] put on users needs to be minimized to preserve usability. Reducing the amount of required knowledge , things a user has to recall , or the number of available choices and necessary decisions are important in this context. This also applies for frequent task switching demands. Also, default configurations should be appropriate and safe to use. Twenty-one publications find that high amounts of *interaction demands* [61, 20, 1, 42, 10, 67, 37, 16, 25, 22, 3, 4, 6, 12, 24, 30, 46, 58, 60, 62, 64] affect usability negatively since users generally favor solutions that don't require significant effort. Necessary interaction should be simple. Integrating security solutions into existing well-known systems reduces required efforts. So does centralized authentication.

Info & Support: This aspect is addressed by the second largest amount of studies. It covers how information should be presented to users. Firstly, it should be highly *comprehensible*[59, 20, 1, 69, 34, 15, 67, 22, 51, 2, 4–6, 9, 12, 27, 28, 31, 33, 40, 41, 49, 55, 57, 58, 66, 70] in both formulation and amount. Low abstraction levels facilitate understanding by non-experts. Reasonable amounts prevent overexertion of users. Furthermore, information needs to be *findable*[59, 20, 1, 15, 67, 22, 21, 28, 41, 49, 55], meaning that users should not have to conduct taxing searches, especially external ones. Information should also be *complete* [59, 34, 4–6, 9, 12, 14, 27, 31, 43, 55, 57] enough to sufficiently address potential problems regarding all functionalities. Explaining *risks & benefits*[59, 11, 22, 51, 9, 12, 21, 23, 26, 28, 55, 60, 70] of security solutions and particular user decisions reduces usability issues and increases trust. Making users aware of threats and consequences helps increasing acceptance of security requirements and enables better system understanding and utilization. *Context related* [65, 59, 22, 6, 21, 28, 55, 62] information corresponds directly to executed tasks and allows to exhibit specifically required actions without the need to interrupt said tasks. This reduces perceived complexity and strain.

Transparency: Systems should be transparent regarding *status and completion*[61, 42, 67, 11, 22, 27, 36, 46, 48–50, 54, 55, 57, 58, 62]. Feedback should be provided about underlying mechanisms, the progress of security actions, the system's status, and task completion. This approach facilitates trust and reduces error rates. Providing knowledge about *available choices*[65, 11, 28, 33] when users need to make important decisions helps them to react properly and reduces error rates.

Time: Secondary only to cognitive load, invested time until successful *task completion*[61, 59, 65, 20, 44, 42, 34, 11, 47, 37, 16, 51, 4, 7, 14, 17–19, 24, 28, 30, 31, 33, 35, 32, 38–40, 46, 49, 53, 54, 56, 58, 64, 66, 68, 70] is one of the most prominent us-

ability aspects. Inefficient time utilization due to delays can impair users' primary objectives and thereby reduce usability significantly. Periods of delay and idle waiting should be minimized. Additionally, putting users under *time pressure* [56, 68] by time-out settings increases error rates and stress levels and reduces perceived usability.

4 Conclusions

This paper aimed to summarize the meaning of usable security by analyzing recently published research to identify the dimensions that encompass the term usable security. Using a structured literature review, this research identified 70 papers from the past five years that discussed the topic of usable security. Using thematic coding, 14 aspects were created from analyzing the included papers, the aspects were then refined into 31 subcategories that describe usability factors for security measures. The most discussed subcategories dictate that the time needed to complete security tasks, the cognitive load added by security tasks and the ease of completing security tasks. While this research does not attempt to weight the different identified aspects, this aligns well with the common understanding of a need for time-efficient and easy-to-use security functions.

The results of this paper is a summary of current research that can help researchers as well as practitioners to better understand the topic of usable security, a necessity in implementing user-centred security measures and applications. It also provides a better understanding of the users roles and challenges in security and can be used as a reference model when developing security functions, applications and procedures. While this research employs measures such as backwards snowballing to be as complete as possible, a given limitation is that it relies on previous research. A possible impact on that is that no previously unknown usability factors has been discovered.

An apparent direction for future work would be to research the identified usability factors from a user-centred standpoint. Such a project could aim to include users in an attempt to weight the different factors according to the users perception. Another direction for future work would be to continue the research by developing concrete guidelines for implementation of user-centered security. Such a project would include practitioners as well as researchers and users.

References

1. * Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M.: Obstacles to the adoption of secure communication tools. 2017 IEEE Symposium on Security and Privacy pp. 137–153 (2017)
2. * Acar, Y., Fahl, S., Mazurek, M.L.: You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In: 2016 IEEE SecDev. pp. 3–8
3. * Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., Reich, C.: Security, privacy and usability–a survey of users' perceptions and attitudes. In: TrustBus 2015. pp. 153–168. Springer (2015)

4. * Al-Sarayreh, K.T., Hasan, L.A., Almakadmeh, K.: A trade-off model of software requirements for balancing between security and usability issues. International Review on Computers and Software **10**(12), 1157–1168 (2015)
5. * Alarifi, A., Alsaleh, M., Alomar, N.: A model for evaluating the security and usability of e-banking platforms. Computing **99**(5), 519–535 (2017)
6. * Almutairi, E., Al-Megren, S.: Usability and security analysis of the keepkey wallet. In: 2019 IEEE ICBC. pp. 149–153
7. * Alshamsi, A., Williams, N., Andras, P.: The trade-off between usability and security in the context of egovernment: a mapping study. In: Proceedings of BCS-HCI 30. pp. 1–13 (2016)
8. * Alshanketi, F., Traore, I., Ahmed, A.A.: Improving performance and usability in mobile keystroke dynamic biometric authentication. In: 2016 IEEE SPW. pp. 66–73. IEEE (2016)
9. * Andriotis, P., Oikonomou, G.C., Mylonas, A., Tryfonas, T.: A study on usability and security features of the android pattern lock screen. Inf. Comput. Security **24**(1), 53–72 (2016)
10. * Atwater, E., Bocovich, C., Hengartner, U., Lank, E., Goldberg, I.: Leading johnny to water: Designing for usability and trust. In: SOUPS 2015 (2015)
11. * Bai, W., Kim, D., Namara, M., Qian, Y., Kelley, P.G., Mazurek, M.L.: Balancing security and usability in encrypted email. IEEE Internet Computing **21**(3), 30–38 (2017)
12. * Bai, W., Namara, M., Qian, Y., Kelley, P.G., Mazurek, M.L., Kim, D.: An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems. In: SOUPS 2016). pp. 113–130 (2016)
13. * Belk, M., Pamboris, A., Fidas, C., Katsini, C., Avouris, N., Samaras, G.: Sweet-spotting security and usability for intelligent graphical authentication mechanisms. In: WIMS 17. pp. 252–259 (2017)
14. * Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., Uebelacker, S.: Maybe poor johnny really cannot encrypt: The case for a complexity theory for usable security. In: NSPW 15p. pp. 85–99 (2015)
15. * Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S.M., Cranor, L.F., Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. In: USEC. Citeseer (2015)
16. * Bindu, C.S.: Secure usable authentication using strong pass text passwords. IJCNIS (2015)
17. * Bošnjak, L., Brumen, B.: Examining security and usability aspects of knowledge-based authentication methods. In: 2019 MIPRO. pp. 1181–1186 (2019)
18. * Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J., Deng, L.: Barriers to usable security? three organizational case studies. IEEE Security Privacy **14**(5), 22–32 (2016)
19. * Carbone, R., Ranise, S., Sciarretta, G.: Design and security assessment of usable multi-factor authentication and single sign-on solutions for mobile applications. In: IFIP International Summer School on Privacy and Identity Management. pp. 51–66. Springer (2018)
20. * Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L.F., Christin, N.: "it's not actually that horrible": Exploring adoption of two-factor authentication at a university. In: CHI '18
21. * Das, S., Dingman, A., Camp, L.J.: Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In: FC 2018. pp. 160–179. Springer (2018)

22. * Das, S., Russo, G., Dingman, A.C., Dev, J., Kenny, O., Camp, L.J.: A qualitative study on usability and acceptability of yubico security key. In: STAST 17. pp. 28–39. ACM (2018)
23. * Das, S., Wang, B., Tingle, Z., Camp, L.J.: Evaluating user perception of multi-factor authentication: A systematic review. arXiv preprint arXiv:1908.05901 (2019)
24. * Ebert, A., Marouane, C., Rott, B., Werner, M.: Keypocket-improving security and usability for provider independent login architectures with mobile devices. In: SecureComm 2015. pp. 41–57. Springer (2015)
25. * Fagan, M., Khan, M.M.H.: Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In: SOUPS 2016. pp. 59–75 (2016)
26. * Feth, D.: User-centric security: optimization of the security-usability trade-off. In: ESEC/FSE 2015. pp. 1034–1037 (2015)
27. * Feth, D., Maier, A., Polst, S.: A user-centered model for usable security and privacy. In: Tryfonas, T. (ed.) HAS 2017. pp. 74–89. Springer (2017)
28. * Feth, D., Polst, S.: Heuristics and models for evaluating the usability of security measures. In: MUC 2019, pp. 275–285 (2019)
29. * Fukumitsu, M., Hasegawa, S., Iwazaki, J., Sakai, M., Takahashi, D.: A proposal of a password manager satisfying security and usability by using the secret sharing and a personal server. In: AINA 2016. pp. 661–668 (2016)
30. * Glass, B., Jenkinson, G., Liu, Y., Sasse, M.A., Stajano, F.: The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions. arXiv preprint arXiv:1607.03417 (2016)
31. * Gordieiev, O., Kharchenko, V.S., Vereshchak, K.: Usable security versus secure usability: an assessment of attributes interaction. In: ICTERI (2017)
32. * Goudalo, W., Kolski, C.: Towards advanced enterprise information systems engineering. In: ICEIS 2016. pp. 400–411 (2016)
33. * Green, M., Smith, M.: Developers are not the enemy!: The need for usable security apis. IEEE Security Privacy **14**(5), 40–46 (2016)
34. * Hasan, L.A., Al-Sarayreh, K.T.: An integrated measurement model for evaluating usability attributes. In: IPAC 2015. ACM (2015)
35. * Hausawi, Y.M., Allen, W.H.: Usable-security evaluation. In: HAS 2015 (2015)
36. * İşler, D., Küpçü, A., Coskun, A.: User perceptions of security and usability of mobile-based single password authentication and two-factor authentication. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 99–117. Springer (2019)
37. * Karapanos, N., Marforio, C., Soriente, C., Capkun, S.: Sound-proof: Usable two-factor authentication based on ambient sound. In: USENIX 2015 (2015)
38. * Katsini, C., Belk, M., Fidas, C., Avouris, N., Samaras, G.: Security and usability in knowledge-based user authentication: A review. In: PCI 16. pp. 1–6 (2016)
39. * Khan, H., Hengartner, U., Vogel, D.: Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In: SOUPS 2015. pp. 225–239 (2015)
40. * Khodadadi, T., Islam, A.K.M.M., Baharun, S., Komaki, S.: Evaluation of recognition-based graphical password schemes in terms of usability and security attributes. International Journal of Electrical and Computer Engineering **6**(6), 2939–2948 (2016)
41. * Krombholz, K., Mayer, W., Schmiedecker, M., Weippl, E.: " i have no idea what i'm doing"-on the usability of deploying {HTTPS}. In: USENIX 2017. pp. 1339–1356 (2017)

42. * Lerner, A., Zeng, E., Roesner, F.: Confidante: Usable encrypted email: A case study with lawyers and journalists. EuroSP 2017 pp. 385–400 (2017)
43. * Ling, Z., Borgeest, M., Sano, C., Lin, S., Fadl, M., Yu, W., Fu, X., Zhao, W.: A case study of usable security: Usability testing of android privacy enhancing keyboard. In: Ma, L., Khreishah, A., Zhang, Y., Yan, M. (eds.) Wireless Algorithms, Systems, and Applications. pp. 716–728. Springer (2017)
44. * Mayron, L.M.: Biometric authentication on mobile devices. IEEE Security Privacy **13**, 70–73 (2015)
45. * McGregor, S.E., Charters, P., Holliday, T., Roesner, F.: Investigating the computer security practices and needs of journalists. In: USENIX 2015). pp. 399–414 (2015)
46. * Melicher, W., Kurilova, D., Segreti, S.M., Kalvani, P., Shay, R., Ur, B., Bauer, L., Christin, N., Cranor, L.F., Mazurek, M.L.: Usability and security of text passwords on mobile devices. In: CHI 2016. pp. 527–539 (2016)
47. * Meng, W., Liu, Z.: Tmgmap: Designing touch movement-based geographical password authentication on smartphones. In: ISPEC 2018. pp. 373–390. Springer (2018)
48. * N, M., P. Onay, D.: A systematic mapping study of usability vs security. In: CEIT 2018. pp. 1–6
49. * Napoli, D.: Developing accessible and usable security (accus) heuristics. In: Extended Abstracts of the CHI 2018. pp. 1–6 (2018)
50. * Naqvi, B., Seffah, A.: Interdependencies, conflicts and trade-offs between security and usability: Why and how should we engineer them? In: HCII 2019. pp. 314–324. Springer (2019)
51. * Nwokedi, U.O., Onyimbo, B.A., Rad, B.B.: Usability and security in user interface design: a systematic literature review. vol. 8, pp. 72–80 (2016)
52. * Oluwafemi, A.J., Feng, J.H.: Usability and security: A case study of emergency communication system authentication. In: Stephanidis, C. (ed.) HCI International 2019. pp. 205–210. Springer International Publishing
53. * Patil, A.D., De Meer, H.: Usability of it-security in smart grids. In: e-Energy 2018. pp. 393–395. ACM (2018)
54. * Qin, L., Lapets, A., Jansen, F., Flockhart, P., Albab, K.D., Globus-Harris, I., Roberts, S., Varia, M.: From usability to secure computing and back again. In: SOUPS 2019) (2019)
55. * Realpe, P.C., Collazos, C.A., Hurtado, J., Granollers, A.: A set of heuristics for usable security and user authentication. In: Interacción '16. pp. 1–8. ACM (2016)
56. * Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., Seamons, K.: A usability study of five two-factor authentication methods. In: SOUPS 2019) (2019)
57. * Reynolds, J., Smith, T., Reese, K., Dickinson, L., Ruoti, S., Seamons, K.: A tale of two studies: The best and worst of yubikey usability. In: 2018 IEEE Symposium on Security and Privacy. pp. 872–888
58. * Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., Zappala, D., Seamons, K.E.: "we're on the same page": A usability study of secure email using pairs of novice users. In: CHI 16 (2016)
59. * Ruoti, S., Andersen, J., Hendershot, T., Zappala, D., Seamons, K.E.: Private webmail 2.0: Simple and easy-to-use secure email. In: UIST '16 (2016)
60. * Ruoti, S., Andersen, J., Monson, T., Zappala, D., Seamons, K.: A comparative usability study of key management in secure email. In: SOUPS 2018). pp. 375–394 (2018)
61. * Ruoti, S., Roberts, B., Seamons, K.E.: Authentication melee: A usability analysis of seven web authentication systems. In: WWW '15 (2015)

62. * Ruoti, S., Seamons, K.E.: Johnny's journey toward usable secure email. IEEE Security Privacy **17**(6), 72–76 (2019)
63. * Sasse, A.: Scaring and bullying people into security won't work. IEEE Security Privacy **13**(3), 80–83 (2015)
64. * Schwab, D., ALharbi, L., Nichols, O., Yang, L.: Picture passdoodle: Usability study. In: IEEE Big Data Service 2018. pp. 293–298 (2018)
65. * Shay, R., Bauer, L., Christin, N., Cranor, L.F., Forget, A., Komanduri, S., Mazurek, M.L., Melicher, W., Segreti, S.M., Ur, B.: A spoonful of sugar?: The impact of guidance and feedback on password-creation behavior. In: CHI 15. pp. 2903–2912. ACM (2015)
66. * Shirvanian, M., Saxena, N.: On the security and usability of crypto phones. In: ACSAC 2015. pp. 21–30 (2015)
67. * Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K.E., Zappala, D.: Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In: SOUPS 2017 (2017)
68. * Wang, T., Ge, H., Chowdhury, O., Maji, H.K., Li, N.: On the security and usability of segment-based visual cryptographic authentication protocols. In: CCS 16. pp. 603–615 (2016)
69. * Weber, S., Harbach, M., Smith, M.: Participatory design for security-related user interfaces. USEC 2015 **15** (2015)
70. * Wolf, F., Kuber, R., Aviv, A.J.: " pretty close to a must-have" balancing usability desire and security concern in biometric adoption. In: CHI 19. pp. 1–12 (2019)
71. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qualitative research in psychology **3**(2), 77–101 (2006)
72. Brooke, J.: Sus-a quick and dirty usability scale. Usability evaluation in industry **189**(194), 4–7 (1996)
73. Das, S., Dingman, A., Camp, L.J.: Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In: FC 2018 (2018)
74. Furnell, S., Esmael, R., Yang, W., Li, N.: Enhancing security behaviour by supporting the user. Computers Security **75**, 1–9 (2018)
75. He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., Ur, B.: Rethinking access control and authentication for the home internet of things (iot). In: USENIX 2018. pp. 255–272 (2018)
76. Jesson, J., Matheson, L., Lacey, F.M.: Doing your literature review: Traditional and systematic techniques. Sage (2011)
77. Khan, H., Hengartner, U., Vogel, D.: Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In: SOUPS 2015. pp. 225–239 (2015)
78. Kitchenham, B.: Procedures for performing systematic reviews. Keele, UK, Keele University **33**(2004), 1–26 (2004)
79. Marchal, S., Armano, G., Gröndahl, T., Saari, K., Singh, N., Asokan, N.: Off-the-hook: An efficient and usable client-side phishing prevention application. IEEE Transactions on Computers **66**(10), 1717–1733 (2017)
80. Meline, T.: Selecting studies for systematic review: Inclusion and exclusion criteria. Contemporary issues in communication science and disorders **33**(21-27) (2006)
81. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX 1999. vol. 348, pp. 169–184 (1999)
82. Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: EASE 14. Citeseer (2014)