Exploring the meaning of Usable Security - a literature review

Journal:	*Information and Computer Security*
Manuscript ID	ICS-10-2020-0167.R1
Manuscript Type:	Original Article
Keywords:	usability, Security, usable security

Exploring the meaning of Usable Security - a literature review

Authors

Affiliations

Abstract

Purpose: For decades, literature has reported on the perceived conflict between usability and security. This mutual trade-off needs to be considered and addressed whenever security products are developed. Achieving well-balanced levels of both is a precondition for sufficient security since users tend to reject unusable solutions. To assess it correctly, usability should be evaluated in the context of security. This paper aims to identify and describe universally applicable and solution-independent factors that affect the perceived usability of security mechanisms.

Design/methodology/approach: The selected methodology was a systematic literature review during which multiple database resources were queried. Application of predefined selection criteria led to the creation of a bibliography before backward snowballing was applied to minimize the risk of missing material of importance. All 70 included publications were then analyzed through thematic analysis.

Findings: The study resulted in the identification of 14 themes and 30 associated sub-themes representing aspects with reported influence on perceived usability in the context of security. While some of them were only mentioned sparsely, the most prominent and thus presumably most significant ones were: simplicity, information and support, task completion time, error rates, and error management.

Originality/value: The identified novel themes can increase knowledge about factors that influence usability. This can be useful for different groups: end-users may be empowered to choose appropriate solutions more consciously, developers may be able to avoid common usability pitfalls when designing new products, and system administrators may benefit from a better understanding of how to configure solutions and how to educate users efficiently.

Keywords: usability, security, usable security

Article Classification: Literature review

Introduction

Owing to the fact that 59% of the world's population is making use of today's Internet (Clement, 2020), it is difficult to imagine how peoples' daily lives could function without it. From mundane tasks such as ordering groceries to holding highly sensitive conversations or executing financial transactions, online services are deeply infused into large portions of human society.

This dependency naturally comes with a corresponding downside: increased risk of becoming a cybercrime victim. According to Clement (2019), 1,244 data breaches exposing 446.5 million information records were registered during 2018 in the USA alone. Such reports illustrate that the implementation of adequate security solutions is crucial. However, according to Fischer-Hübner *et al*. (2010), user-reluctance to utilize such solutions constitutes a common hinder. Therefore, they emphasize the necessity to consider usability aspects when security solutions are developed. In a similar context, Hof (2015) states that this is hard to accomplish since all users possess different experience levels which can complicate the task of assessing usability objectively. It is also emphasized that a security mechanism never should restrict the users' primary task. Instead of creating

hinders, security experts should recognize human limitations and refrain from trying to bully users into barely usable systems (Sasse, 2015).

Despite the dire need for effective security solutions that are usable enough to be readily adopted, the current situation still leaves much to be desired. Hof (2015) expresses that usable security often is merely the afterthought of another afterthought (security). Additionally, literature frequently describes a distinct trade-off between security and usability (e. g. Cranor and Buchler, 2014; Bai *et al.,* 2016; Feth, 2015; Naqvi *et al*., 2019). Said conflict is what this study will address. The purpose will be to approach the outlined issues by identifying common factors that can affect the usability of security solutions and thus facilitate the creation of more usable ones. This papers expands on Lennartson *et al*. (2020).

The applied method will be a systematic literature review. Multiple databases will be queried with relevant search terms. The resulting bibliography of contending publications will be screened via predefined selection criteria. The whole procedure is inspired by the recommendations of Kitchenham (2004). To avoid missing relevant publications, backward snowballing (Wohlin, 2014) will be conducted as a complementary search method. All included publications will finally be analyzed via thematic analysis (Braun and Clarke, 2006).

Results will outline how the scientific community nowadays perceives usable security and the trade-off between its two conflicting factors.

Background

More than 20 years ago, Whitten and Tygar (1999) identified and exposed distinct difficulties regarding the relation between usability and security. They emphasized that those properties often are in conflict with each other and that mutual trade-offs are commonplace. Since then, similar notions have been expressed repeatedly. A typical opinion is that usability has to be sacrificed to achieve sufficient security (Cranor and Buchler, 2014). Fagan and Khan (2016) declared that users often put usability before security, exposing themselves to increased risks. They stated that such decisions are frequently made despite being aware of existing dangers. Moreover, Benenson et al. (2015) found that no large-scale success had yet been achieved in the endeavor of providing sufficiently usable security solutions.

The international standard ISO 9241-11:2018 (International Standards Organization [ISO], 2018) defines the term usability as

”*the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.*”

This interpretation appears to be too generalized and topic-unrelated to cover all facets of the aforementioned conflict since the implications of usability vary when put into different contexts (Whitten and Tygar, 1999). Also, a better fitting context could motivate users to reassess their security behavior (Fagan and Khan, 2016). Thus, to provide one that fits said trade-off, a less generalized and more security-focused perspective on usability is necessary. This paper intends to provide such a perspective by identifying the crucial attributes of usable security.

Research aim

To assess the previously described conflict’s impact on security solutions, it is necessary to understand which properties are capable of facilitating, respectively hindering, usability. Such knowledge can enable improved remediation approaches that are specifically adapted to the delineated trade-off; it is thus highly relevant to the realm of information security. Hence, this paper’s aim of research is to identify and describe critical factors that affect the usability of security solutions.

Such knowledge can be valuable for different groups: developers will be able to better predict how end-users perceive and utilize products. Also, it will be easier for them to avoid common usability pitfalls during the development phase. System administrators will gain a better understanding of how

to approach and educate end-users, and how to configure security solutions to provide sufficient usability. End-users can profit from an increased insight that allows to pick appropriate solutions more consciously.

Methodology

The utilized scientific method to accomplish the aim of research will be a systematic literature review as described by Kitchenham (2004). A systematic literature review allows to review and summarize the current state of research regarding particular phenomena (Kitchenham, 2004); phenomena like the usability-security conflict.

To ensure replicability and allow readers to assess the applied method, parameters like utilized resources and search terms should be predefined (Kitchenham, 2004). To avoid missing important publications, multiple databases ought to be queried (Brereton et al., 2007).

All search terms will be applied to all databases. While the first two resources are suggested by Brereton et al. (2007), resources 3 to 7 are both deemed relevant as well as freely accessible to the authors.

Utilized resources:

- *ACM Digital Library*
- *IEEExplore*
- *Springer Link*
- *dblp*
- *ArXiv*
- *SCOPUS*
- *CSCAN HAISA*

Applied search terms:

- *"usable security"*
- *usability AND security*

Kitchenham (2004) stated that "*The basis for the selection of primary studies is the inclusion and exclusion criteria. The criteria should be developed beforehand, to avoid bias.*" (p. 47). Selection criteria will be used to assess the suitability of publications in regard to the study's aim.

Inclusion criteria:

- *IC1: Published between 2015 and 2020*
- *IC2: Published in peer-reviewed journal or conference*

- *IC3: Publication is relevant to the topic*
- *IC4: Written in English, Swedish or German*

Remark to IC4: English is chosen since it is the most common language for research communication. Swedish and German is included since the authors are fluent in them.

Exclusion criteria:

- *EC1: Publication occurs multiple times*
- *EC2: Fails to meet inclusion criteria*
- *EC3: Payment required for access*
- *EC4: Incomprehensible description of method or result*

Once the initial search is conducted, a complementary search method will be applied to avoid missing additional material of importance. Said method, backward snowballing, involves the application of selection criteria to all references of already included publications (Wohlin, 2014).

After completion of both search stages, included publications will be analyzed through thematic analysis as described by Braun and Clarke (2006). According to their proposed stages, included publications will be read in their entirety before passages of apparent relevance will be highlighted. Those sections will then be evaluated to identify significant patterns. Said patterns will be refined until they resemble themes that are suitable to address the study's aim. During this process, the software tool MAXQDA will be used to facilitate manual work. Its inclusion will not affect the conducted procedure and study outcome. It will merely be used to simplify and accelerate the act of creating, archiving, and assessing codes.

This study will be subject to some distinct limitations. Firstly, search terms will only be applied to titles and keywords. Secondly, the period of acceptable publications will be restricted to the last five years. This ensures that only the most recent research will be incorporated into the results, ensuring an outcome that illustrates the current state of the art. Even if important earlier papers might be excluded, presenting a complete assembly of all previous research is out of scope for this work. Lastly, this work will not address concerns of User Experience Design (UXD), a realm that primarily deals with the task of providing users with comfortable experiences in terms of design, function but also usability (Interaction Design Foundation, n.d.). While there is a certain overlap between UXD and usable security, UXD will not be considered further since it fails to supply a sufficient security context.

Research ethics will be maintained by avoiding to present citations and statements in flawed contexts that are removed from their original implications. Since matters of information security in public are touched, external ethical aspects will be affected as well. However, even if malicious actors might be interested in utilizing the study's outcome, the risk that this actually enables exploitation is judged to be exceedingly low. Results will only illustrate properties that affect the perceived usability of security solutions. As violations of ethical values are improbable, the study's potential benefits justify its publication.

Practical Selection Process

In this subchapter, the results from the selection process are presented. This is done in table 1 (below) which should be read per stage from left to right.

Table 1: Practical selection process when the aforementioned methodology was executed

Stage	Resource	Search Date	Hits	Eliminated due to							Included
				EC1		EC2		EC3		IC3	
I. Initial Search	*ACM Dig. Lib.*	2020-01-02	12	145		159		15		10	**49**
	IEEExplore	2020-01-02	68								
	Springer Link	2020-01-02	14								
	dblp	2020-01-02	142								
	ArXiv	2020-01-02	20								
	SCOPUS	2020-01-11	102								
	CSCAN HAISA	2020-01-03	20								
II. Backward Snowballing	References of included publications from stage I	2020-01-16	1641	IC1	IC2	IC3	IC4	EC1	EC3	EC4	**21**
				1250	161	147	1	57	3	1	
	FINAL BIBLIOGRAPHY										**70**

Results

The outlined selection process created a bibliography of 70 primary studies. In reference to thematic analysis as proposed by Braun and Clarke (2006), all were read in their entirety to increase familiarity. Afterward, initial codes were created by highlighting apparently relevant passages. Those were then evaluated regarding significant recurring patterns applicable for clustering codes into preliminary themes. Themes and affiliated codes were then further refined to ensure relevance to the study's aim. MAXQDA was used to simplify the practical work of parsing the bibliography, highlighting passages, creating colored codes, and organizing those into themes.

All primary studies were assigned an identifier to map them to affiliated themes. Identifiers were ranging from A01 to A49 when accepted during the initial search, and S01 to S21 when accepted during backward snowballing. Table 2 (below) depicts said allocation.

Table 2: Identifiers assigned to primary studies

ID	Publication	ID	Publication	ID	Publication
A01	Al Abdulwahid et al. (2015)	A25	Green and Smith (2016)	A49	Wolf et al. (2019)
A02	Acar et al. (2016)	A26	Hausawi and Allen (2015)	S01	Shay et al. (2015)
A03	Al-Sarayreh et al. (2015)	A27	Isler et al. (2019)	S02	Ruoti et al. (2015)
A04	Alarifi et al. (2017)	A28	Katsini et al. (2016)	S03	Ruoti, S., Andersen, J., Hendershot, T., Zappala, D., & Seamons, K. (2016)

Table 2, continuation

ID	Publication	ID	Publication	ID	Publication
A05	Almutairi and Al-Megren (2019)	A29	Khan et al. (2015)	S04	Colnago et al. (2018)
A06	Alshamsi et al. (2016)	A30	Khodadadi et al.(2016)	S05	Mayron (2015)
A07	Alshanketi et al. (2016)	A31	Krombholz et al. (2017)	S06	Abu-Salma et al. (2017)
A08	Andriotis et al. (2016)	A32	Ling et al. (2017)	S07	Lerner et al. (2017)
A09	Bai et al. (2016)	A33	Melicher et al. (2016)	S08	Weber et al. (2015)
A10	Belk et al. (2017)	A34	Merdanoglu and Durdu (2018)	S09	Hasan and Al-Sarayreh (2015)
A11	Benenson et al. (2015)	A35	Napoli (2018)	S10	Bhagavatula et al. (2015)
A12	Bošnjak and Brumen (2019)	A36	Naqvi and Seffah (2019)	S11	Atwater et al. (2015)
A13	Caputo et al. (2016)	A37	Oluwafemi and Feng (2019)	S12	Vaziripour et al. (2017)
A14	Carbone et al. (2018)	A38	Patil and Meer (2018)	S13	Bai et al. (2017)
A15	Das, S., Dingman, A., & Camp, L. J. (2018)	A39	Qin et al. (2019)	S14	Sasse (2015)
A16	Das et al. (2019)	A40	Realpe et al. (2016)	S15	Meng and Liu (2018)
A17	Ebert et al. (2015)	A41	Reese et al. (2019)	S16	Karapanos et al. (2015)
A18	Feth (2015)	A42	Reynolds et al. (2018)	S17	McGregor et al. (2015)
A19	Feth et al. (2017)	A43	Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., . . . Seamons, K. E. (2016)	S18	Bindu (2015)
A20	Feth and Polst (2019)	A44	Ruoti et al. (2018)	S19	Fagan and Khan (2016)
A21	Fukumitsu et al. (2016)	A45	Ruoti and Seamons. (2019)	S20	Das, S., Russo, G., Dingman, A. C., Dev, J., Kenny, O., & Camp, L. J. (2018)
A22	Glass et al. (2016)	A46	Schwab et al. (2018)	S21	Nwokedi et al. (2016)
A23	Gordieiev et al. (2017)	A47	Shirvanian and Saxena (2015)		
A24	Goudalo and Kolski (2016)	A48	Wang et al. (2016)		

A thorough examination of codes revealed 14 emerging themes representing aspects that affect usability. After further assessment, those were divided into 30 sub-themes representing prominent factors. Table 3 (below) displays affiliations between themes and publications.

Table 3: Themes, related sub-themes, and publications (quantity in parentheses)

Themes	Sub-themes	Affiliated Publications
Cost of Use	Resource Consumption	S06 (1)
	Financial	S06, S09, S19 (3)
Consistency	Implementation	A05, A40, A42 (3)
	Behavior	S09, A23 (2)

Table 3, continuation

Themes	Sub-themes	Affiliated Publications
Perception	Trust & Reputation	S02, S06, S11-S13, S17, S19, A03, A27, A44 (10)
	Coolness Factor	S02 (1)
GUI	Adjustable	A03, A23, A40 (3)
	Understandable & Simple	S03, S08, S09, S21, A04, A30, A34, A35, A39, A40, A42, A47 (12)
Scalability	Key Handling	A09 (1)
	Account Handling	S20, A17, A42 (3)
Compatibility	Security Solutions	S06 (1)
	Systems & Services	S04, S06, S20, A17, A42 (5)
Adaptability	User Capacity	S09, S21, A04, A09, A13, A19, A20, A28, A35, A40, A49 (11)
	User Control	S04, S08, S20, A20, A23, A30, A35, A40 (8)
Interference	Physical	S02, S10, A41, A42 (4)
	Re-authentication	A01, A05, A11, A17, A19, A29 (6)
	Workflow	S04, S14, A18, A19, A22, A35, A38 (7)
Error Rate	S04, S09, S14, S16, A01, A03, A12, A15, A18, A25-A30, A38, A42, A43, A47-A49 (21)	
Error Management	Recovery	S04, S09, S20, A03, A07, A09, A11, A21, A30, A35, A36, A39, A40, A42 (14)
	Prevention	S03, S04, S08, S09, S12, A03, A05, A20, A23, A25, A34, A35, A39, A40, A42 (15)
Simplicity	Cognitive Load	S05, S07, S09-S14, S17, S20, S21, A01, A02, A04, A05, A06, A08, A09-A11, A14, A15, A17, A18, A20, A22, A23, A25, A27, A29-A31, A35, A37, A38-A40, A42, A44-A47 (42)
	Interaction Demands	S02, S04, S06, S07, S11, S12, S16, S18-S20, A01, A03, A05, A09, A17, A22, A33, A43-A46 (21)
Info & Support	Comprehensible	S03, S04, S06, S08-S10, S12, S20, S21, A02-A05, A08, A09, A15, A19, A20, A23, A25, A30, A31, A35, A40, A42, A43, A47, A49 (28)
	Findable	S03, S04, S06, S10, S12, S20, A15, A31, A35, A40 (10)
	Context Related	S01, S03, S20, A05, A15, A20, A40, A45 (8)
	Risks & Benefits	S06, S13, S20, S21, A08, A09, A15, A16, A18, A20, A40, A44, A49 (13)
	Complete	S03, S09, A03-A05, A08, A09, A11, A19, A23, A32, A40, A42 (13)
Transparency	Status & Completion	S02, S07, S12, S13, S20, A19, A20, A27, A33-A36, A39, A40, A42, A43, A45 (17)
	Available Choices	S01, S13, A20, A25 (4)
Time	Time Pressure	A41, A48 (2)
	Task Completion	S01-S05, S07, S09, S13, S15, S16, S18, S21, A03, A06, A11-A14, A17, A20, A22-A26, A28-A30, A33, A35, A38, A39, A41, A43, A46-A49 (38)

The defined themes can be described as follows:

Cost of Use: This theme addresses factors that users tend to perceive as inconvenient in terms of cost-effectiveness. While purely *financial* costs are mentioned repeatedly, one publication (S06) states that even *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*, meaning that similar tasks are supposed to be working identically, and *implementation*. The latter includes standardized setups (A42), consistent phrasing (A40), and design that allows to easily recognize requirements and conditions (A05).

Perception: Willingness to adopt security solutions depends partially on how they are perceived by individuals. The most prominent aspect relates to *trust and reputation*. Multiple studies report that users prefer solutions they feel confident with. Such beliefs arise when a solution is from reputable sources (A44, S12), verified by experts (A27), or recommended by mouth-to-mouth propaganda (S06, S11). Additionally, the *coolness factor* of authentication schemes might be another contributing aspect (S02). Usually, different and innovative approaches are seen as "cooler" than traditional ones.

GUI (Graphical User Interface): This theme is concerned with the way the GUI is constructed. The first sub-theme implies that it should be *understandable and simple*. This includes visualization of navigation options and clear menu arrangements (A04) in accordance to what users might anticipate (A35). Also, the GUI should not require unnecessary user attention (A30) and merely display information necessary for decision making (A40). Moreover, S03 and S08 report advantages of distinct color schemes. A GUI that is *adjustable* to the user's preferences increases usability (A03, A23, A40) since it improves learnability (A03).

Scalability: Another affecting trait is the extent to which security solutions can deal with multiple user accounts and security keys. Usable *account handling* does not restrict the number of applicable user accounts (A17) and allows to operate multiple accounts with mutual keys (S20). Also, some users desire account sharing capabilities with other individuals (A42). Concerning *key handling*, a scalable solution should be able to install and control multiple keys without complicating usage (A09).

Compatibility: Security solutions should be compatible with commonly used *systems and services* to be perceived as usable. This includes operating systems (A42) and third-party services like email tools (S04). The trend of developing new security solutions with separate and fragmented user bases constitutes a significant hinder to usability (S06). Compatibility with other *security solutions* is crucial since users will presumably reject overly incompatible products (S06) 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 sub-theme deals with the amount of allowed *user control*. Enabling users to customize configurations to their preferences increases convenience (A20, A23). This includes optical appearances and the possibility to create shortcuts for frequent tasks (A40). Forcing users to follow strict default configurations is detrimental to usability (S04). Facilitating memorability by allowing users to choose their own passwords is advantageous (A30). Regarding *user capacity*, security solutions should be adaptable to various expertise levels (A04, A13, A19, A35, A40, S21,A49). Intelligently adapting solutions would be beneficial (A28). Furthermore, solutions should also adapt to users' disabilities (S09, A04, A20, A35).

Interference: Usability is hampered when users' primary tasks are disturbed. The first sub-theme addresses *workflow* interference. Task complication via too restrictive security measures

should be avoided (A18, A19, A22) while natural workflow should be preserved (A35, A38, S14). Necessary security actions should be arranged in ways that minimize interruptions (S04). Even *re-authentication* requests are described as disruptive and inconvenient (A01). They might be perceived as wasted time (A05) and cause increased complexity (A17). Also, compelling users to remember passwords repeatedly interrupts other tasks since enforced context switches may cause confusion (A11). Unpredictable re- authentication requests can cause significant annoyance (A29). Finally, there is a *physical* aspect to this theme. Users are anxious to lack immediate access to physical tokens when needed (A41, A42). Fear of loss or theft is common (S02). Additionally, inherent weaknesses such as difficulties working in dark or wet environments can reduce usability (S10) and thus impair security when users revert to more insecure practices.

Error rate: To which extent a security solution enables users to conduct their primary task without having to deal with annoying completion failures is a salient usability precondition. Increasing error rates cause substantial inconvenience since users are forced to repeat actions. Solutions become ineffective when they are unable to complete tasks as intended (A26, A28). In this context, it is secondary if errors are caused directly by the system or indirectly via users (S04). Direct errors relate to inherent system flaws like interruptive false negatives (A47) or failure to successfully encrypt plaintext (A43). Indirect errors are often caused by aspects like excessive complexity (A03, A18, A42). When security solutions are error-prone, users may choose to circumvent them to preserve usability (A01).

Error management: Effective means of *prevention* are required to reduce error rates. Users should be provided with clear and simple instructions that help to prevent frequent errors (S04). Incorrect operations can be prevented by automatic means such as input validity checks (A03, A23, S09). Before errors occur, easy-to-understand warning messages should be communicated clearly (A05, A25, A42, S09, S12) and point out problem causes (A20). Making users aware of their actions' negative consequences beforehand is beneficial (A40, S08). If such hints go unheeded, execution should be rejected (A40). If errors cannot be prevented, proper means of error *recovery* should exist to maintain usability. One way to recover is to allow users to cancel or revert their actions (A40, A42, A09). Laborious recovery procedures are harmful to usability (A11). Giving simple hints about causes and recommended actions is preferable (A30, A40). Users should be empowered to address most errors without external help (A11, S04), but it should still be available if needed (A40).

Simplicity: A great number of studies report that users become overwhelmed by overly complex systems. Several papers stress that the *cognitive load* put on users needs to be minimized to preserve usability. Reducing the amount of required knowledge (A02, A25, A31, A39, A47, S09), things a user has to recall (A01, A27, A46), or the number of available choices and necessary decisions (A05, A10, A15) are important in this context. This also applies to frequent task switching demands (A11). One pivotal concept to relieve end-users from burdening complexity is to implement automation (A02, A09, A45, S07, S10, S11, S12). Better task ordering can reduce task switching strains (A22, A31). Also, default configurations should be appropriate and safe to use (A25, A31, A35, A40). Twenty-one publications find that high amounts of *interaction demands* affect usability negatively since users generally favor solutions that don't require significant effort. Necessary interaction should be simple (A33). Integrating security solutions into existing well-known systems reduces required efforts (A43, A45, S04, S07, S11). So does centralized authentication (A01, A17, S02).

Info & Support: This theme is addressed by the second-largest amount of studies. It covers how information should be presented to users. Firstly, it should be highly *comprehensible* in both formulation and amount. Low abstraction levels facilitate understanding by non-experts (A04, A19, S06, S08). Reasonable amounts prevent overexertion of users (A02, A20, A35). Furthermore, information needs to be *findable*, meaning that users should not have to conduct

taxing searches, especially external ones (A31). Thus, the implementation of text-search functions is helpful (A35). Information should also be *complete* enough to sufficiently address potential problems regarding all functionalities. If integrated information proves to be insufficient, providing additional support is beneficial (A11, A40). Explaining *risks & benefits* 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 (A18, S20) and enables better system understanding and utilization (A44, A49, S13). *Context related* information corresponds directly to executed tasks and allows to exhibit specifically required actions (A45) without the need to interrupt said tasks (A20). This reduces perceived complexity and strain (S01, S20).

Transparency: Systems should be transparent regarding *status and completion*. Feedback should be provided about underlying mechanisms (A19), the progress of security actions (A20, A45), the system's status (A40, A42), and task completion (A35). This approach facilitates trust (A27, A36, A43, S13) and reduces error rates (A33). Likewise, keeping users in the dark may seriously harm usability (A39). Hence, users tend to prefer transparent systems (S02). Providing knowledge about *available choices* when users need to make important decisions helps them to react properly (A20, A25) and reduces error rates (S01).

Time: Secondary only to cognitive load, invested time until successful *task completion* is one of the most prominent usability aspects. Inefficient time utilization due to delays can impair users' primary objectives and thereby reduce usability significantly (A13). Frustration occurs quickly if users sense that their time is wasted (A33). Hence, periods of delay and idle waiting should be minimized (A11, A23, S13). Invested time must be recognized as a precious resource (A20) to maintain usability and to ensure continued system adaption (A49). Additionally, putting users under *time pressure* by time-out settings increases error rates (A41) and stress levels (A48). None of that will be advantageous to perceived usability.

Discussion

The results reinforce the perception that the conflict between usability and security still exists (Naqvi et al., 2019). Manipulation of the identified aspects will tip the balance in favor of either usability or security, but rarely both. Just as reported by Whitten and Tygar (1999), those traits remain contrasting opposites.

This illustrates one of the major challenges in information security: while usability in other contexts can be treated as an independent goal, security contexts demand to consider it in relation to its impact on security. The task of finding a balance that provides satisfying levels of both is therefore of paramount importance when it comes to the development of security solutions. As a result, there are practical limitations as to how much security is feasible before usability is hampered enough that users are chased away.

Usable security is often addressed from the perspective of specific security solutions/techniques. This review adapted a more comprehensive and solution-independent approach. Its primary scientific contribution is the identification, description, and presentation of universal usability characteristics that can be utilized for future research, regardless if of equally broad or narrower scope. The applied measures to ensure validity should allow it to be used as a valid foundation.

To prevent bias in the form of misunderstandings or misinterpretations by the authors, a strictly transparent and reproducible methodology was applied. Multiple resources and search terms, as well as backward snowballing, were utilized to avoid missing relevant material. Only peer- reviewed publications were included to ensure sufficient quality.

Readers can profit from increased knowledge about the usability trade-off and its characteristics: end-users might be empowered to avoid unusable solutions whereas developers and administrators might be able to better predict and meet the expectations of end-users. Ultimately, such deeper insight

may prevent security hazards caused by irritated users who circumvent security. Since no previously unpublished sensitive information is disclosed, the review's ethical impact is considered negligible and hence outweighed by the aforementioned practical benefits.

Conclusions

After applying the previously explained methodology, the aim of research was reached by identifying a comprehensive set of aspects affecting usability in a security context. Compiling and describing those aspects represents the work's main contribution. Figure 1 (below) depicts their distribution.

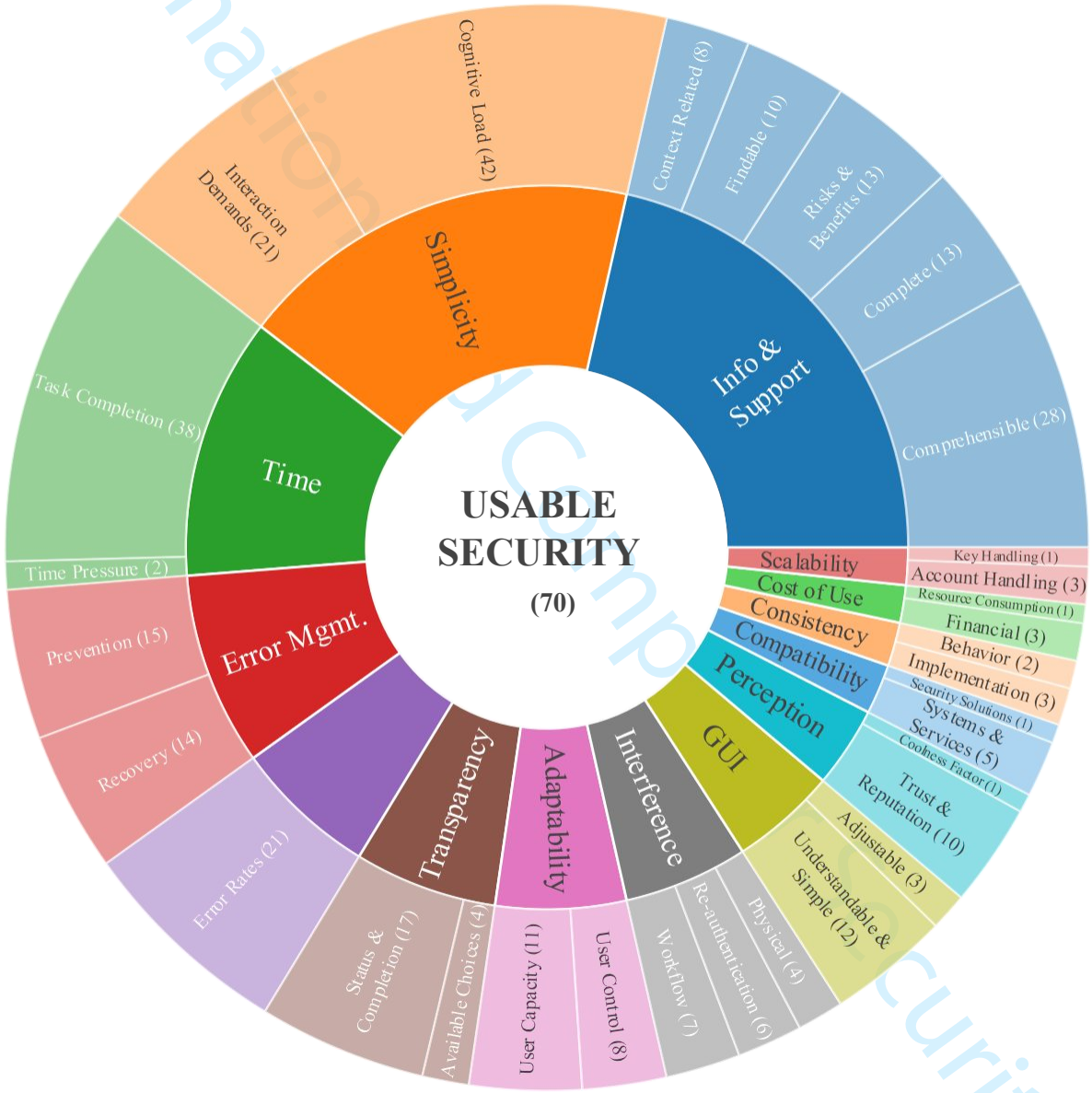

Figure 1: Hierarchical model of aspects with impact on usable security. Parentheses depict the quantity of relating publications. Varying colors are used to separate the different aspects; aside from that, they do not signify any deeper meaning.

While the applicability of identified characteristics might vary in relation to different use cases and security solutions, all of them should be considered regardless of their frequency of occurrence in order to approach the outlined conflict holistically. However, while the mere quantity of publications affiliated with particular themes may not constitute an expressive measure in itself, its proportion

should not be disregarded since large numbers indicate increased impact. In this respect, the review implies that some aspects appear to be especially significant: *simplicity*, *info & support*, *task completion time*, *error rates,* and *error management*. Similarly, sparsely mentioned ones like *coolness factor* or *resource consumption* might not be equally crucial.

This study revealed distinct interrelations between identified themes. For example, error rates increase with high complexity or imposed time pressure, interference raises complexity and aggravates time for task completion, and sufficient transparency is capable of enhancing user perception. Then again, automation and transparency need to be kept in balance since too much automation reduces trust and too much transparency increases complexity. Presumably, there are a lot more cases of such mutual influence, making usable security a complicated matter to understand and approach. Therefore, practitioners should not only address individual usability aspects but consider their interrelations as well.

While this study indicated that individual usability aspects can affect each other strongly, deeper implications of that discovery were not investigated further. A meaningful topic for future research and a logical next step in the quest to mitigate the security-usability trade-off would hence be to examine such interrelations in more detail, and how they can be aligned to achieve desirable results. A second direction for future work would be to research the users preferences in regards to the usability aspects identified in this paper.

References

Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017), "Obstacles to the Adoption of Secure Communication Tools", in *SP 2017*, IEEE, pp. 137-153.

Acar, Y., Fahl, S., & Mazurek, M. L. (2016), "You are not your developer, either: A research agenda for usable security and privacy research beyond end users", in *SecDev 2016,* IEEE, pp. 3-8.

Al Abdulwahid, A., Clarke, N., Stengel, I., Furnell, S., & Reich, C. (2015), "Security, privacy and usability–a survey of users' perceptions and attitudes", in *TrustBus 2015,* Springer, pp. 153-168.

Alarifi, A., Alsaleh, M., & Alomar, N. (2017), "A model for evaluating the security and usability of e-banking platforms", *Computing,* Vol. 99 No. 5, pp. 519-535.

Almutairi, E., & Al-Megren, S. (2019), "Usability and Security Analysis of the KeepKey Wallet", in *ICBC 2019,* IEEE, pp. 149-153.

Al-Sarayreh, K. T., Hasan, L. A., & Almakadmeh, K. (2015), "A trade-off model of software requirements for balancing between security and usability issues", *International Review on Computers and Software,* Vol. 10 No. 12, pp. 1157-1168.

Alshamsi, A., Williams, N., & Andras, P. (2016), "The trade-off between usability and security in the context of eGovernment: a mapping study", in *HCI'16,* BCS, pp. 1-13.

Alshanketi, F., Traore, I., & Ahmed, A. A. (2016), "Improving performance and usability in mobile keystroke dynamic biometric authentication", in *SPW 2016,* IEEE, pp. 66-73.

Andriotis, P., Oikonomou, G. C., Mylonas, A., & Tryfonas, T. (2016), "A study on usability and security features of the Android pattern lock screen", *Inf. & Comput. Security,* Vol. 24 No. 1, pp. 53-72.

Atwater, E., Bocovich, C., Hengartner, U., Lank, E., & Goldberg, I. (2015), "Leading Johnny to water: Designing for usability and trust", in *SOUPS 2015,* USENIX, pp. 69-88.

Bai, W., Kim, D., Namara, M., Qian, Y., Kelley, P. G., & Mazurek, M. L. (2017), "Balancing security and usability in encrypted email", *IEEE Internet Computing,* Vol. 21 No. 3, pp. 30-38.

Bai, W., Namara, M., Qian, Y., Kelley, P. G., Mazurek, M. L., & Kim, D. (2016), "An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems", in *SOUPS 2016,* USENIX, pp. 113-130.

Belk, M., Pamboris, A., Fidas, C., Katsini, C., Avouris, N., & Samaras, G. (2017), "Sweet-spotting security and usability for intelligent graphical authentication mechanisms", in *WI'17,* ACM, pp. 252-259.

Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., & Uebelacker, S. (2015), "Maybe poor johnny really cannot encrypt: The case for a complexity theory for usable security", in *NSPW'15*, ACM, pp. 85-99.

Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., & Savvides, M. (2015), "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption", in *Proc. USEC,* Internet Society, pp. 1-10.

Bindu, C. S. (2015), "Secure usable authentication using strong pass text passwords", *IJ Computer Network and Information Security*, *7*(4), 57-64.

Bošnjak, L., & Brumen, B. (2019), "Examining Security and Usability Aspects of Knowledge-based Authentication Methods", in *MIPRO 2019,* IEEE, pp. 1181-1186.

Braun, V., & Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative research in psychology*, Vol. 3 No. 2, pp. 77-101.

Brereton, P., Kitchenham, B. A., Budgen, D., Turner, M., & Khalil, M. (2007), "Lessons from applying the systematic literature review process within the software engineering domain", *Journal of systems and software,* Vol. 80 No. 4, pp. 571-583.

Caputo, D. D., Pfleeger, S. L., Sasse, M. A., Ammann, P., Offutt, J., & Deng, L. (2016), "Barriers to Usable Security? Three Organizational Case Studies". *IEEE Security & Privacy,* Vol. 14 No. 5, pp. 22-32.

Carbone, R., Ranise, S., & Sciarretta, G. (2018), "Design and Security Assessment of Usable Multi-factor Authentication and Single Sign-On Solutions for Mobile Applications - A Workshop Experience Report", in *IFIP 2018,* Springer, pp. 51-66.

Clement, J. (2019), "Cyber crime: number of breaches and records exposed 2005-2018", available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (accessed 11 February 2020).

Clement, J. (2020). "Worldwide digital population as of January 2020", available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed 11 February 2020).

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L. F., & Christin, N. (2018), ""It's not actually that horrible": Exploring Adoption of Two-Factor Authentication at a University, in *CHI'18,* ACM, pp. 1-11.

Cranor, L. F., & Buchler, N. (2014), "Better together: Usability and security go hand in hand", *IEEE Security & Privacy*, Vol. 12 No. 6, pp. 89-93.

Das, S., Dingman, A., & Camp, L. J. (2018), "Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key", in *FC 2018,* Springer, pp. 160-179.

Das, S., Russo, G., Dingman, A. C., Dev, J., Kenny, O., & Camp, L. J. (2018), "A qualitative study on usability and acceptability of Yubico security key", in *STAST'17,* ACM, pp. 28-39.

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019), "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review", in Furnell, S., & Clarke, N. (Eds.), *HAISA 2019,* CSCAN, pp. 166-178.

Ebert, A., Marouane, C., Rott, B., & Werner, M. (2015), "KeyPocket - Improving Security and Usability for Provider Independent Login Architectures with Mobile Devices", in *SecureComm 2015,* Springer, pp. 41-57.

Fagan, M., & Khan, M. M. H. (2016), "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice", in *SOUPS 2016,* USENIX, pp. 59-75.

Feth, D. (2015), "User-centric security: optimization of the security-usability trade-off", in *ESEC/FSE'15,* ACM, pp. 1034-1037.

Feth, D., Maier, A., & Polst, S. (2017), "A User-Centered Model for Usable Security and Privacy", in Tryofanos, T. (Ed.), *HAS 2017*, Springer, pp. 74-89.

Feth, D., & Polst, S. (2019), "Heuristics and Models for Evaluating the Usability of Security Measures", in *MuC'19,* ACM, pp. 275-285.

Fischer-Hübner, S., Iacono, L. L., & Möller, S. (2010), "Usable security und privacy", *Datenschutz und Datensicherheit-DuD*, Vol. 34 No. 11, pp. 773-782.

Fukumitsu, M., Hasegawa, S., Iwazaki, J., Sakai, M., & Takahashi, D. (2016), "A Proposal of a Password Manager Satisfying Security and Usability by Using the Secret Sharing and a Personal Server", in *AINA 2016,* IEEE, pp. 661-668.

Glass, B., Jenkinson, G., Liu, Y., Sasse, M. A., & Stajano, F. (2016), "The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions", in *EuroUSEC 2016,* Internet Society.

Gordieiev, O., Kharchenko, V. S., & Vereshchak, K. (2017), "Usable Security Versus Secure Usability: an Assessment of Attributes Interaction", in *ICTERI 2017,* Springer, pp. 727-740.

Goudalo, W., & Kolski, C. (2016), "Towards Advanced Enterprise Information Systems Engineering - Solving Resilience, Security and Usability Issues within the Paradigms of Socio-Technical Systems", in *ICEIS 2016,* SCITEPRESS, pp. 400-411.

Green, M., & Smith, M. (2016), "Developers are Not the Enemy!: The Need for Usable Security APIs", *IEEE Security & Privacy,* Vol. 14 No. 5, pp. 40-46.

Hasan, L. A., & Al-Sarayreh, K. T. (2015), "An integrated measurement model for evaluating usability attributes", in *IPAC'15,* ACM, pp. 1-6.

Hausawi, Y. M., & Allen, W. H. (2015), "Usable-security evaluation", in *HAS 2015*, Springer, pp. 335-346.

Hof, H. J. (2015), "User-centric IT security-how to design usable security mechanisms", *arXiv preprint arXiv:1506.07167*.

Interaction Design Foundation (n.d.), "User Experience (UX) Design", available at: https://www.interaction-design.org/literature/topics/ux-design (accessed 27 march 2020).

Isler, D., Küpçü, A., & Coskun, A. (2019), "User Perceptions of Security and Usability of Mobile-Based Single Password Authentication and Two-Factor Authentication", in *DPM/CBT 2019,* Springer, pp. 99-117.

ISO (2018), "ISO 9241-11:2018(en), Ergonomics of human-system interaction", available at: https://www.iso.org/obp/ui/#iso:std:iso:9241:-11:ed-2:v1:en (accessed 13 February 2020)

Karapanos, N., Marforio, C., Soriente, C., & Capkun, S. (2015), "Sound-proof: usable two-factor authentication based on ambient sound", in *USENIX Security'15,* USENIX, pp. 483-498.

Katsini, C., Belk, M., Fidas, C., Avouris, N., & Samaras, G. (2016), "Security and usability in knowledge-based user authentication: A review", in *PCI'16,* ACM, pp. 1-6.

Khan, H., Hengartner, U., & Vogel, D. (2015), "Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying", in *SOUPS 2015,* USENIX, pp. 225-239.

Khodadadi, T., Islam, A. K. M. M., Baharun, S., & Komaki, S. (2016), "Evaluation of recognition-based graphical password schemes in terms of usability and security attributes", *International Journal of Electrical and Computer Engineering,* Vol. 6 No. 6, pp. 2939-2948.

Kitchenham, B. (2004), "Procedures for performing systematic reviews", *Keele University, Vol. 33*, pp. 1-26.

Krombholz, K., Mayer, W., Schmiedecker, M., & Weippl, E. R. (2017), ""I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS", in *USENIX Security'17,* USENIX, pp. 1339-1356.

Lennartsson, M., Kävrestad, J., & Nohlberg, M. (2020). Exploring the Meaning of "Usable Security". In *International Symposium on Human Aspects of Information Security and Assurance* (pp. 247-258). Springer, Cham.

Lerner, A., Zeng, E., & Roesner, F. (2017), "Confidante: Usable encrypted email: A case study with lawyers and journalists", in *EuroS&P 2017,* IEEE, pp. 385-400.

Ling, Z., Borgeest, M., Sano, C., Lin, S., Fadl, M., Yu, W., ... & Zhao, W. (2017), "A case study of usable security: Usability testing of android privacy enhancing keyboard", in *WASA 2017,* Springer, pp. 716-728.

Mayron, L. M. (2015), "Biometric Authentication on Mobile Devices", *IEEE Security & Privacy,* Vol. 13, pp. 70-73.

McGregor, S. E., Charters, P., Holliday, T., & Roesner, F. (2015), "Investigating the computer security practices and needs of journalists", in *USENIX Security'15,* USENIX, pp. 399-414.

Melicher, W., Kurilova, D., Segreti, S. M., Kalvani, P., Shay, R., Ur, B., . . . Mazurek, M. L. (2016), "Usability and Security of Text Passwords on Mobile Devices", in *CHI'16,* ACM, pp. 527-539.

Meng, W., & Liu, Z. (2018), "TMGMap: designing touch movement-based geographical password authentication on smartphones", in *ISPEC 2018,* Springer, pp. 373-390.

Merdanoglu, N., & Durdu, P. O. (2018), "A systematic mapping study of usability vs security", in *CEIT 2018,* IEEE, pp. 1-6.

Napoli, D. (2018), "Developing Accessible and Usable Security (ACCUS) Heuristics", in *CHI EA'18,* ACM, pp. 1-6.

Naqvi, B., & Seffah, A. (2019), "Interdependencies, Conflicts and Trade-Offs Between Security and Usability: Why and How Should We Engineer Them?", in *EWHCI 2019,* Springer, pp. 314-324.

Nwokedi, U. O., Onyimbo, B. A., & Rad, B. B. (2016), "Usability and security in user interface design: a systematic literature review", *IJITCS*, Vol. 8 No. 5, pp. 72-80.

Oluwafemi, A. J., & Feng, J. H. (2019), "Usability and Security: A Case Study of Emergency Communication System Authentication", in *EWHCI 2019,* Springer, pp. 205-210.

Patil, A. D., & Meer, H. d. (2018), "Usability of IT-Security in Smart Grids", in *e-Energy'18,* ACM, pp. 393-395.

Qin, L., Lapets, A., Jansen, F., Flockhart, P., Albab, K. D., Globus-Harris, I., . . . Varia, M. (2019), "From Usability to Secure Computing and Back Again", In *SOUPS 2019,* USENIX, pp. 191-210.

Realpe, P. C., Collazos, C. A., Hurtado, J., & Granollers, A. (2016), "A Set of Heuristics for Usable Security and User Authentication", in *Interacción'16,* ACM, pp. 1-8.

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. E. (2019), "A Usability Study of Five Two-Factor Authentication Methods", in *SOUPS 2019,* USENIX, pp. 357-370.

Reynolds, J., Smith, T., Reese, K., Dickinson, L., Ruoti, S., & Seamons, K. (2018), "A tale of two studies: The best and worst of yubikey usability", in *SP 2018,* IEEE, pp. 872-888.

Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., . . . Seamons, K. E. (2016), ""We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users", in *CHI '16,* ACM, pp. 4298-4308.

Ruoti, S., Andersen, J., Hendershot, T., Zappala, D., & Seamons, K. (2016), "Private Webmail 2.0: Simple and easy-to-use secure email", in *UIST'16,* ACM, pp. 461-472.

Ruoti, S., Andersen, J., Monson, T., Zappala, D., & Seamons, K. E. (2018), "A Comparative Usability Study of Key Management in Secure Email", in *SOUPS 2018,* USENIX, pp. 375-394.

Ruoti, S., Roberts, B., & Seamons, K. (2015), "Authentication melee: A usability analysis of seven web authentication systems", in *WWW'15,* ACM, pp. 916-926.

Ruoti, S., & Seamons, K. E. (2019), "Johnny's Journey Toward Usable Secure Email", *IEEE Security & Privacy,* Vol., 17 No. 6, pp. 72-76.

Sasse, A. (2015), "Scaring and bullying people into security won't work", *IEEE Security & Privacy,* Vol. 13 No. 3, pp. 80-83.

Schwab, D., ALharbi, L., Nichols, O., & Yang, L. (2018), "Picture PassDoodle: Usability Study", in *BigDataService 2018,* IEEE, pp. 293-298.

Shay, R., Bauer, L., Christin, N., Cranor, L. F., Forget, A., Komanduri, S., ... & Ur, B. (2015), "A spoonful of sugar? The impact of guidance and feedback on password-creation behavior", in *CHI'15,* ACM, pp. 2903-2912.

Shirvanian, M., & Saxena, N. (2015), "On the Security and Usability of Crypto Phones", in *ACSAC 2015,* ACM, pp. 21-30.

Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K., & Zappala, D. (2017), "Is that you, Alice? a usability study of the authentication ceremony of secure messaging applications", in *SOUPS 2017,* USENIX, pp. 29-47.

Wang, T., Ge, H., Chowdhury, O., Maji, H. K., & Li, N. (2016), "On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols", in *CCS'16,* ACM, pp. 603-615.

Weber, S., Harbach, M., & Smith, M. (2015), "Participatory design for security-related user interfaces", in *Proc. USEC,* Internet Society.

Whitten, A., & Tygar, J. D. (1999), "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0", in *USENIX Security'99,* USENIX, pp. 169-184.

Wohlin, C. (2014), "Guidelines for snowballing in systematic literature studies and a replication in software engineering", in *EASE'14,* ACM, p. 38.

Wolf, F., Kuber, R., & Aviv, A. J. (2019), ""Pretty Close to a Must-Have": Balancing Usability Desire and Security Concern in Biometric Adoption", in *CHI'19,* ACM, pp. 1-12.

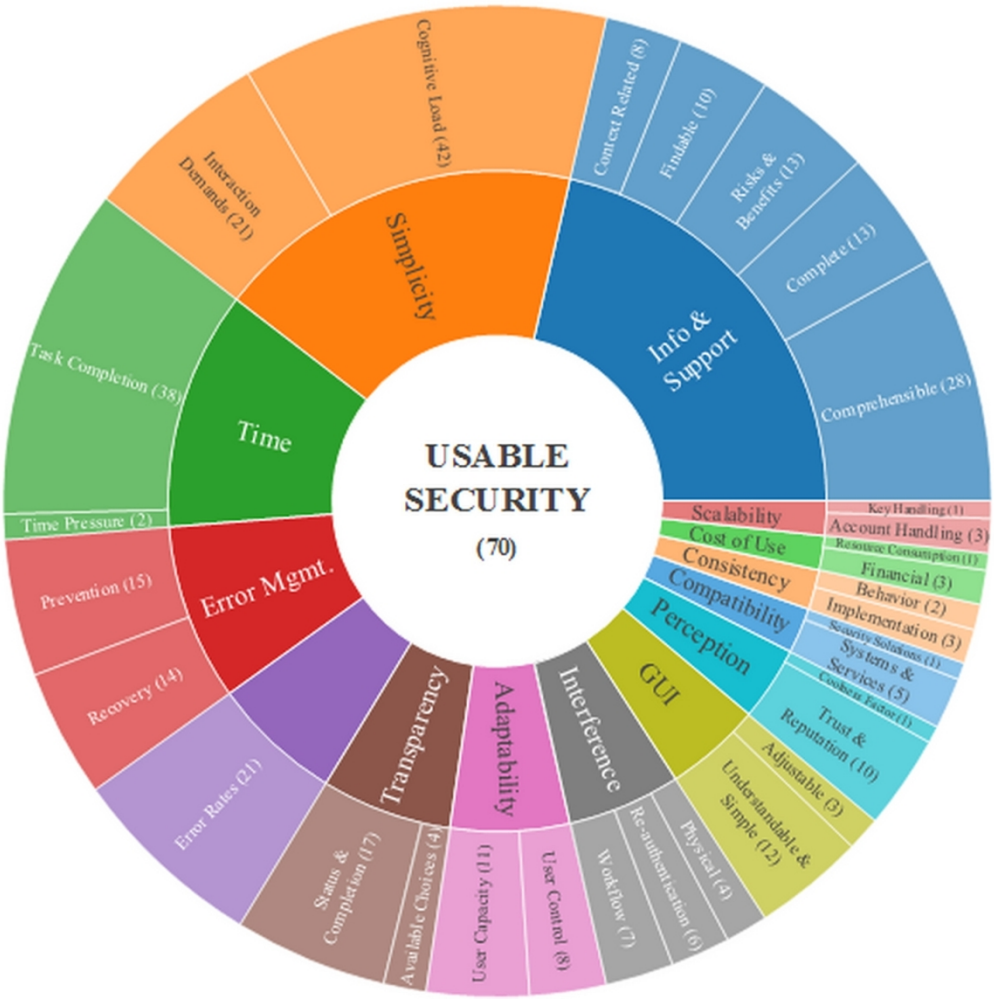

Figure 1: Hierarchical model of aspects with impact on usable security. Parentheses depict the quantity of relating publications. Varying colors are used to separate the different aspects; aside from that, they do not signify any deeper meaning.

200x199mm (254 x 254 DPI)