Guidelines for Usable Cybersecurity: Past and Present

Jason R. C. Nurse, Sadie Creese, Michael Goldsmith, Koen Lamberts
University of Warwick
Coventry, CV4 7AL, UK
{j.nurse, s.creese, m.h.goldsmith, k.lamberts}@warwick.ac.uk

***Abstract*—Usability is arguably one of the most significant social topics and issues within the field of cybersecurity today. Supported by the need for confidentiality, integrity, availability and other concerns, security features have become standard components of the digital environment which pervade our lives requiring use by novices and experts alike. As security features are exposed to wider cross-sections of the society, it is imperative that these functions are highly usable. This is especially because poor usability in this context typically translates into inadequate application of cybersecurity tools and functionality, thereby ultimately limiting their effectiveness. With this goal of highly usable security in mind, there have been a plethora of studies in the literature focused on identifying security usability problems and proposing guidelines and recommendations to address them. Our paper aims to contribute to the field by consolidating a number of existing design guidelines and defining an initial core list for future reference. Whilst investigating this topic, we take the opportunity to provide an up-to-date review of pertinent cybersecurity usability issues and evaluation techniques applied to date. We expect this research paper to be of use to researchers and practitioners with interest in cybersecurity systems which appreciate the human and social elements of design.**

***Index Terms*—Cybersecurity; system usability; usable security; guidelines and recommendations; social cybersecurity issues**

I. Introduction

Security and usability have often been regarded as competing system goals [1]. In [2], the authors have even posed the question: Is usable security an oxymoron? A classic example of the contrasting aims of these two concepts can be seen when dealing with passwords, one of the most commonly used security mechanisms today. From a security perspective, long, complex (hard to guess), unique passwords which are changed regularly is ideal, however, from a usability viewpoint, these requirements are often a major strain on users and in turn, a system's usability [3, 4]. A majority of these general security issues are also present in the cybersecurity context, where the emphasis is on the digital environment. The challenge faced by the Cybersecurity Usability and comparable Human-Computer Interaction and Security (HCISec/HCI-S) fields therefore, is bridging that conceptual and application gap, and emphasising the need to fuse these two concepts thereby creating usable cybersecurity interfaces and systems. This is especially as security features and functions become standard components in software applications and end-user systems. Common examples of these user-facing applications and systems include, word processing software (with tasks such as adding digital signatures to facilitate subsequent document authentication), document readers (which allow setting viewing, access and printing permissions), personal devices (with activities such as applying security pins and locks to mobile phones), personal security firewalls and email encryption tools. All of these relate to typical tasks in the cyberspace environment.

In this paper, we aim to recap some of the major developments in the Cybersecurity Usability and HCISec domains, particularly as they relate to guidance and recommendations for highly usable cybersecurity systems. As such, one of the key contributions of this paper is its consolidation of existing work and outline of an initial core list of general guidelines. While we do appreciate specific guidance given in areas such as authentication, access control, encryption, firewalls, secure device pairing and secure interaction (e.g., [3, 5–13]), at this stage we concentrate more on *general* and therefore largely context-independent guidelines. A list focused at that general level is necessary as it will form a central part of future work, which amongst other things, includes assessing the applicability (and possible targeting) of guidelines to the ISO 27002 [14] range of security controls. We also envisage that this list may have a broader value external to our direct intentions, as it supplies a useful state-of-the-art review for academics, IT professionals and system designers.

To achieve the research aim above, this paper is divided into three sections. Section II reflects on usability as an important social issue within cybersecurity. Here, we outline a number of core usability problems and emphasise the need for usable security within cyberspace. Next, Section III briefly reviews common techniques being used to evaluate the usability of cybersecurity interfaces and systems. This section provides a useful resource on evaluation methods and the areas in which they have been applied to date. In Section IV, we then consolidate several of the main general guidelines proposed in the literature applicable to usable cybersecurity. This pulls together a number of key research articles and recommendations and allows us to define an initial core list. The final section then concludes this paper and discusses avenues for future work.

II. Cybersecurity and Usability: What are the problems?

As mentioned in the previous section, cybersecurity and usability often tend to be regarded as competing goals.

Within the literature, there are numerous examples where cybersecurity systems have been criticised for poor usability. Drawing from work in [15], there are six categories of usability studies in the field generally. These encompass authentication, encryption, Public Key Infrastructure (PKI), device pairing, security tools and security systems. In each of these areas, problems have been documented which affect the usability of cybersecurity interfaces and functionality. Apart from system usability being a problem in itself for users (in terms of confusion, frustration, and so on), a critical point to note is that poor usability in a cybersecurity context typically translates into inaccurate or inadequate configurations of security tools and functionality (e.g., access controls, firewalls, encryption mechanisms, routers) and/or users subverting security features all together ([16–19]). Both of these activities are likely to have significant negative impacts on the security state of respective systems and associated networks. Below, we review some of the most salient articles and problems faced to the usable cybersecurity domain.

Authors in [16] provide one of the seminal articles on usable security (with some focus on encryption) and introduce several of the main issues faced by users. They expressed that interfaces for security tend to be confusing and clumsy, and therefore hinder, as opposed to assist users — a situation arguably still present today as papers are still forthcoming (e.g., [4, 19, 20]) targeting these and similar issues. According to [16], this usability problem is exacerbated by a number of properties implicit to security. These properties include: users are unmotivated (security is usually a secondary goal), abstraction (security is governed by underlying abstract rules, such as security policies), lack of feedback (providing quality feedback is difficult noting security's complex nature), barn door property (if a secret is left unprotected even for a short time, there is no way to be sure that an attacker has not reached it), and weakest link (a security chain is as strong as its weakest link, and all users need to understand this fact as it relates to the security of their systems).

In another research study, this time around authentication mechanisms, the authors [3] posit that passwords provide numerous challenges for users. In various cases for example, users have to use and remember several passwords, interact with multiple password policies (requirements and conditions) and various different systems. The end result is a significant strain on users' limited working memories. Memorability, user knowledge and motivation are some of the core issues highlighted in that work that affect security aspects and their usability. Work by [5] supplies another useful perspective on these issues and the need for user-centred design of security mechanisms.

Further to the problems mentioned above, task workload and increasing complexity of cybersecurity systems has also been cited as noteworthy hindrances to usability [21]. This is even the case for security administrators and developers, individuals that are likely to have undergone some level of training in system application and use. In [22], one can see numerous of these difficulties being discussed as researchers work towards improving the performance of online cybersecurity analysts through visualisation and defensible recommendations. Other research has also expressed the perspective that users face difficulties because of near-impossible system demands on them and secondly, arguably, what users may deem as awkward behaviour (e.g., constantly locking the computer screen when not at one's desk, even for short periods, and the social implications of this action) [23].

The underlying process of systems design as it relates to usability and security has also been discussed. In [6] for example, the author assesses the numerous conflicts between usability and security in design (e.g., bolting on security at the end of design and the reality that this harms usability) and use (e.g., security typically interrupts users from fulfilling immediate usage goals while usability has fulfilling these goals as its aim). Instead of concluding that systems cannot focus on both aspects, [6] stresses that security and usability are key, and the goal should be to consider them early on, iteratively and in concert. Reference [24] is a more recent article that appreciates these issues and looks again towards a user-centric design approach to usable cybersecurity.

Research by [25] also supports the argument for usable cybersecurity systems as he focuses on the problem of a lack of visibility of security functionality in end-user applications. Common failings include, security options fractured across different menus and sub-options, security features listed as 'advanced' (portraying that only advanced users should access them), and lacking visible indicators of system security status. In [20], the author supplies another useful review of cybersecurity usability problems faced by normal end-users. These problems encompass abundance of technical terminology, unclear and confusing functionality, lack of visible system status and informative feedback, forcing uninformed security decisions, and lack of integration of security functionality. Within the article, the author supplies examples of each of these problems in real-world office systems, however there are various other works (e.g., [12, 19, 26, 27]) that support the general argument and exemplify usability problems in security interfaces and systems, from firewalls and network configurations to authentication and encryption mechanisms. With several of the core challenges to the usability of cybersecurity interfaces and systems reviewed, next we consider common methods used in the literature to evaluate these cybersecurity interfaces and systems in terms of their usability.

III. How is Cybersecurity Usability Being Evaluated?

Similar to the general system usability field (e.g., [28]), there are two major methods for evaluating the usability of cybersecurity systems. These approaches are, user studies and expert-based evaluations [29, 30]. In the first of these methods, a representative sample of users is recruited to participate in experiments to test a system's usability. Specific examples of user studies include laboratory-based user testing, questionnaires, interviews, and observing users and recording and assessing system use. Normally this can be structured

around predefined tasks of interest to persons conducting the study.

Various examples of user studies can be found in the cybersecurity literature. From as early as [16] for example, laboratory-based tests have been applied to evaluate how easily users are able to complete predefined security (in this case, encryption-related) tasks. Work by [2] is also another source of research that has drawn upon user testing of cybersecurity applications. There, some of the main techniques mentioned include observations (through one-way mirrors), mirroring the user's screen, questionnaires and semi-structured interviews. In [29], the authors emphasise the importance of user observation in particular, and stress that monitoring is how most usability problems are discovered. To attain as rich a data set as possible, their study also utilises pre/post questionnaires to gauge user progress and 'think aloud' sessions where users are asked to commentate as they perform tasks on the system. Semi-structured interviews are preferred in [12] for evaluation, primarily because of the view that interviews are particularly appropriate for investigating events that happen irregularly and infrequently. Other recent works worthy of note that utilise and discuss these methods include [22, 27, 31, 32].

Within the expert-based evaluation technique, usability experts assess and inspect usability aspects of a system using their knowledge and a range of usability rules and heuristics (rules of thumb) [28]. In this area, cognitive walkthroughs (where evaluators step through a system looking for areas that may negatively affect usability) and heuristic evaluations (testing a system against a set of usability rules) are two of the most prevalent methods [30]. Further examples of the use of heuristic evaluations are apparent in [33] where the authors assess a personal firewall according to HCI-S criteria, and in [34] where the evaluation of security tool alerts is based on preset security usability rules. A perfect example and discourse of the cognitive walkthrough technique is supplied in [30] as the article examines the usability of forensic analysis cybersecurity software. Expert-based methods such as cognitive walkthrough have also been used alongside user studies to enhance evaluations. Work by [16] provides a quick reference of an article that employs this method and laboratory-based tests with the aim of drawing on the strengths of both techniques.

With appreciation of the mixture of techniques in [16] and possible advantages to be gained by combining evaluation methods, we briefly compare user studies and expert-based evaluations. One of the first points to note is that as user studies employ potential system users (and therefore are more likely to replicate actual user behaviour), they are typically regarded as the ideal evaluation method [30]. Furthermore, user studies such as observations, interviews and questionnaires provide rich sources of data that can be analysed in detail for insight and further guidance. The drawback with these methods however, is that they can be time-consuming and expensive [30]. Necessary tasks include finding willing participants, setting up experiments and data gathering tools and software (may also require purchasing software applications and systems or renting usability labs), and finally, conducting the analysis of the qualitative and/or quantitative data collected.

Switching focus to expert evaluation, advantages accompanying this technique include, (i) it uses knowledgeable individuals with some notable level of expertise in usability, (ii) ideally, experts will have a good understanding of the users that the system targets and how they are likely to use the system, and (iii) it directly allows one to focus on a list of high-priority usability principles during system assessment [16, 28]. Possibly the most useful way to combine the two general techniques can be seen in [29]. In their article, the authors highlight that expert-based techniques may be used in the initial stages to guide system design, while user studies might be employed later to confirm design choices and test for usability problems which may have been overlooked. Considering the benefits possible with this joint technique, it will likely be a prime candidate for most future evaluations in the Cybersecurity Usability and HCISec fields.

Having covered several of the problems faced in the usability of cybersecurity systems and interfaces, and prevalent techniques for usability evaluation, we now consider the resulting guidelines that have been proposed. Here we focus on the most significant and relevant guidelines and recommendations which arise from the literature to combat the usability issues presented.

IV. Guidelines for Usable Cybersecurity

To determine the most appropriate guidelines in line with this research's aims, we first searched the literature for *general* recommendations proposed to improve the usability of cybersecurity interfaces and systems. Once found, we defined a preliminary list of guidelines for analysis. Next, we assessed the list by comparing recommendations across the articles and where possible we grouped very similar guidelines, renaming groupings as appropriate. During our analysis, we also noted reoccurring guidelines within these research works (these are shown below in brackets using each guideline's reference listings). In some ways, recommendations that reoccur may be seen as possessing stronger cases of support—we revisit this in future work discussions in Section V. Below we present the refined list of general guidelines drawn from the literature based on our study and analysis.

- *Cybersecurity usability should be considered early on* — Cybersecurity, usability and the interaction between these concepts should be debated and assessed in the initial stages of a system's design and development. Bolting on or retrofitting cybersecurity usability only at the end of a system's development is likely to be detrimental to the system overall and lead to additional usability and security issues. ([6, 35])
- *Accommodate all types of users* — Cybersecurity functionality should be designed such that it is flexible and accommodating to novice and expert users. Whilst novice users may need assistance and step-by-step guidance at times, expert users should be able to quickly access required functionality via system shortcuts, hot keys and

such. In general, this guidance emphasises the need for various ways of system interaction. ([19, 20])

- *Give informative feedback* — A key ingredient to several of the other guidelines for usable cybersecurity below (e.g., help, error handling and visibility of security system state) is useful system feedback. Feedback should be clear, informative, sufficient, not too technical and where appropriate, give suggestions for going forward. ([19,36])
- *Provide help, advice and documentation* — When necessary, users should be able to easily locate and view help and advice manuals and system documentation for cybersecurity functions. If users cannot find, and determine how to use these features, they are likely to be avoided. ([20, 36])
- *Error prevention, handling and recovery/Undo* — Systems should be designed such that they anticipate user errors and prevent against them. If errors do occur however, they should be handled gracefully, be presented in informative prompts and outline steps for recovery. This guideline also suggests that cybersecurity interface designs support undo and quick exit functionalities for when users make mistakes and enter unwanted application states. Users should be able to rely on and not feel at a loss within the application. ([16, 19, 20, 33, 36])
- *Allow for visibility of system state* — Users should be made aware of the current security state of the system. In many ways this is a form of passive feedback of cybersecurity. Some simple examples include, the word 'Secured' on some encrypted or password-protected documents, active icons when security functions are being executed on a system, and padlocks within browsers to indicate browsing using Secure Sockets Layer (SSL)/Transport Layer Security (TLS). ([20, 33, 36])
- *Make security functionality visible and accessible* — Similar to other application features, security should be visible and easily accessed. Hiding cybersecurity functionality within advanced or disparate parts of an interface are likely to make the user's task more difficult and ultimately hamper system usability. ([20, 33])
- *Reduce cognitive load associated with system activities* — Cybersecurity interfaces should be designed to minimise a user's cognitive load whilst using the system. Over the years, various studies on human cognition have highlighted limitations in working memory and the need to support users and work within their memory and thought restrictions. This might include, automating security actions or configurations, ease of system security setup, and generally not placing unreasonable demands on users' memory. Related to cognition, there are a number of general perception and communication aspects that should also be considered when discussing cybersecurity. Reference [37] provides an overview of this field and proposes several recommendations. ([19, 38])
- *Give guidance on what tasks users need to perform and where necessary, provide recommendations support* — Systems need to make users aware of and where necessary, supply them with guidance on the cybersecurity tasks they need to perform. Another part of this guidance is recommendations support where users are unsure of decisions and their implications. Making individuals aware and giving guidance relates to both user domains i.e., systems for security experts (in [22] for example, there is a heavy focus on recommendations and respective justifications), and those for end-users where security is usually a secondary goal. ([16, 36, 38])
- *Emphasise a positive system experience and good levels of user satisfaction* — As much as is feasible, cybersecurity interfaces should aim to provide users with a positive and satisfactory experience. This might consist of activities such as making small interface changes to benefit user preferences or allowing for some degree of security interface/action customisation. ([16, 19, 33, 35])
- *Aesthetic and minimalistic design* — Although it is accepted that some aspects of cybersecurity functionality (e.g., configurations) might be somewhat complex, especially for a novice user, designers should aim to keep interfaces simple, reduce likelihood of information overload, and avoid awkward interface setups. ([33])
- *Design for learnability* — Cybersecurity interfaces should be easy to learn. In [39], learnability is thought to be affected by familiarity and consistency amongst other things. As it relates to cybersecurity, key aspects which might increase usability therefore involve, the use of metaphors (relating the real-world to system functions to exploit familiarity) and consistent terms and dialogues in the system (to avoid confusion). ([33])
- *Reduce use of technical and security-specific terms and jargon* — To use security features, users have to be able to understand what they mean. As such, designers should use technical and security-specific terms sparingly and where they are used, consider giving descriptions. This is particularly useful for end-user systems and novice users. ([20])
- *Facilitate the creation of an accurate mental model* — A mental model can be defined as a user's internal representation or understanding of a system and how it works [39]. Designers should attempt to define systems that consider a user's mental model, and therefore foster the creation of models that accurately represent the cybersecurity interface and functionality. ([36])
- *Design security into all application layers* — Contrary to focusing on security only at the lower and more technical levels of the networking stack, a useful approach might be to design security into all of an application's layers, especially its upper layers. The idea behind this recommendation is to make the underlying security implicit in a user's tasks and generally, their high-level goals. By providing this seamlessness, the system may benefit by being seen as more user-friendly. For this approach to be successful, designers will need to possess a good understanding of users' mental models and how they reason about the system. ([35])

- *Design such that security does not reduce performance* — While maintaining the balance between cybersecurity and usability, system performance is another key aspect. Designers should utilise efficient algorithms and careful design to ensure that security features can be efficiently used within the software application and system. ([20])
- *Tools are not solutions* — Tools including SSL and Internet Protocol Security (IPsec) are building blocks and not solutions to user problems by themselves. To compliment these and other lower level tools, there is a need for high-level building blocks that can be drawn upon by system designers to create more user-focused applications which incorporate usable security. ([35])
- *Separate distinct concepts* — Mixing different concepts may lead to confusion. It may therefore be useful to separate user values from security policies, and also security policies from security implementation. This removes the need for end-users to be well versed in security mechanisms just to create respective and suitable policies. Furthermore, automation of the policy-to-implementation step is one action that would aid significantly in a user's system configuration task. ([19])
- *Note that security management interfaces may need additional usability considerations* — In cybersecurity management interfaces, security is no longer a secondary goal. As such, there are a few other aspects specific to usable cybersecurity that have proven themselves worthy of consideration. These include, ability to assess a cybersecurity system from varying encapsulation levels, facilitating understanding and diagnosis of potential threats, and encouraging management staff to respond to serious security issues promptly [22, 36]. References [40, 41] are sources for other considerations and design guidelines (around usability and otherwise).

V. Conclusion and Future Work

In this paper, we reviewed the Cybersecurity Usability and HCISec fields particularly in terms of core problems faced, evaluation methods to date, and lastly general guidelines proposed. In addition to providing a topical review of key articles within this space, this paper contributes to research by consolidating several existing usability design guidelines applicable to cybersecurity and defining an initial core list for future reference. We expect this list to be of use to researchers and practitioners with interest in designing and creating cybersecurity systems which appreciate the human and social aspect.

Drawing on the research review in this article, we have identified several directions of interest for future work. One such avenue which was hinted at earlier, involves assessing the applicability of the guidelines listed to the general set of security controls in ISO 27002 [14]. This ISO standard (along with others in the ISO 27000 series) is a core point of reference to IT/cybersecurity practitioners and therefore evaluating and if necessary, proposing extended guidance in the usability of these controls is an important aspect. Another direction for future research is the further examination of the support for and importance of specific cybersecurity usability guidelines. This analysis would be conducted with the goal of creating a possible evidence rating or even priority structure for guidelines. Research by [42] is an example of work that has a similar aim (albeit a different context) as it defines and rates Web design and usability guidelines in terms of strength of evidence and relative importance. The ability to draw on these types of ratings is particularly important when balancing cybersecurity and usability, a task that will be crucial for years to come.

Acknowledgment

This work was conducted as a part of the TEASE project, a collaboration between the University of Warwick, HW Communications Ltd and Thales UK Research and Technology. The project is supported by the UK Technology Strategy Board's Trusted Services Competition (www.innovateuk.org) and the Research Councils UK Digital Economy Programme (www.rcuk.ac.uk/digitaleconomy).

References

[1] J. Sherwood, A. Clark, and D. Lynas, *Enterprise security architecture: a business-driven approach*. CMP Books, 2005.

[2] A. J. DeWitt and J. Kuljis, "Is usable security an oxymoron?" *Interactions*, vol. 13, no. 3, pp. 41–44, 2006.

[3] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the weakest link' – a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001.

[4] M. F. Theofanos and S. L. Pfleeger, "Guest editors' introduction: Shouldn't all security be usable?" *IEEE Security and Privacy*, vol. 9, pp. 12–17, 2011.

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

[6] K.-P. Yee, "Aligning security and usability," *Security & Privacy*, vol. 2, no. 5, pp. 48–55, 2004.

[7] T. Whalen, D. Smetters, and E. F. Churchill, "User experiences with sharing and access control," in *CHI'06 extended abstracts on Human factors in Computing Systems*. ACM, 2006, pp. 1517–1522.

[8] S. Sheng, L. Broderick, J. Hyland, and C. Koranda, "Why johnny still can't encrypt: evaluating the usability of email encryption software," in *Symposium On Usable Privacy and Security*, 2006.

[9] M. Sweikata, G. Watson, C. Frank, C. Christensen, and Y. Hu, "The usability of end user cryptographic products," in *Information Security Curriculum Development Conference*. ACM, 2009, pp. 55–59.

[10] R. Kainda, I. Flechais, and A. W. Roscoe, "Usability and security of out-of-band channels in secure device pairing protocols," in *5th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009.

[11] A. Kobsa, R. Sonawalla, G. Tsudik, E. Uzun, and Y. Wang, "Serial hookups: a comparative usability study of secure device pairing methods," in *5th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009.

[12] F. Raja, K. Hawkey, P. Jaferian, K. Beznosov, and K. S. Booth, "It's too complicated, so I turned it off!: expectations, perceptions, and misconceptions of personal firewalls," in *3rd ACM workshop on Assurable and usable security configuration*, 2010, pp. 53–62.

[13] C. Weir, G. Douglas, T. Richardson, and M. Jack, "Usable security: User preferences for authentication methods in ebanking and the effects of experience," *Interacting with Computers*, vol. 22, no. 3, pp. 153–164, 2010.

[14] International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC), "ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management," 2005.

[15] R. Kainda, I. Flechais, and A. W. Roscoe, "Security and usability: Analysis and evaluation," in *International Conference on Availability, Reliability and Security (ARES)*. IEEE, 2010, pp. 275–282.

[16] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," in *8th USENIX Security Symposium*, 1999, pp. 169–184.

[17] S. W. Smith, "Humans in the loop: Human-computer interaction and security," *Security & Privacy, IEEE*, vol. 1, no. 3, pp. 75–79, 2003.

[18] A. L. Stephano and D. P. Groth, "Useable security: interface design strategies for improving security," in *3rd International Workshop on Visualization for Computer Security*. ACM, 2006, pp. 109–116.

[19] C. Kuo, A. Perrig, and J. Walker, "Security configuration for non-experts: A case study in wireless network configuration," in *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. IGI Global, 2009, pp. 179–195.

[20] S. Furnell, "Security usability challenges for end-users," in *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. IGI Global, 2009, pp. 196–219.

[21] M. A. Sasse, "Usability and trust in information systems," *Cyber Trust & Crime Prevention Project*, 2004.

[22] J. Rasmussen, K. Ehrlich, S. Ross, S. Kirk, D. Gruen, and J. Patterson, "Nimble cybersecurity incident management through visualization and defensible recommendations," in *7th International Symposium on Visualization for Cyber Security (VizSec)*. ACM, 2010, pp. 102–113.

[23] M. A. Sasse and I. Flechais, "Usable security: Why do we need it? how do we get it?" in *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly, 2005, pp. 13–30.

[24] C. A. Fidas, A. G. Voyiatzis, and N. M. Avouris, "When security meets usability: A user-centric approach on a crossroads priority problem," in *14th Panhellenic Conference on Informatics*. IEEE, 2010, pp. 112–117.

[25] S. Furnell, "Why users cannot use security," *Computers & Security*, vol. 24, no. 4, pp. 274–279, 2005.

[26] B. D. Payne and W. K. Edwards, "A brief introduction to usable security," *IEEE Internet Computing*, pp. 13–21, 2008.

[27] N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," *Computers & Security*, vol. 30, no. 4, pp. 208 – 220, 2011.

[28] S. Rosenbaum, "Usability evaluations versus usability testing: When and why?" *IEEE Transactions on Professional Communication*, vol. 32, no. 4, pp. 210–216, 1989.

[29] S. Chiasson, P. C. van Oorschot, and R. Biddle, "A usability study and critique of two password managers," in *15th USENIX Security Symposium*, 2006, pp. 1–16.

[30] D. J. Bennett and P. Stephens, "A cognitive walkthrough of autopsy forensic browser," *Information Management & Computer Security*, vol. 17, no. 1, pp. 20–29, 2009.

[31] F. Raja, K. Hawkey, and K. Beznosov, "Revealing hidden context: improving mental models of personal firewall users," in *5th Symposium on Usable Privacy and Security (SOUPS)*. ACM, 2009, pp. 1–12.

[32] P. Shi, H. Xu, and X. Zhang, "Informing security indicator design in web browsers," in *2011 iConference*. ACM, 2011, pp. 569–575.

[33] J. Johnston, J. H. P. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers & Security*, vol. 22, no. 8, pp. 675–684, 2003.

[34] T. Ibrahim, S. Furnell, M. Papadaki, and N. Clarke, "Assessing the usability of end-user security software," in *Trust, Privacy and Security in Digital Business*, ser. Lecture Notes in Computer Science, S. Katsikas, J. Lopez, and M. Soriano, Eds. Springer, 2010, vol. 6264, pp. 177–189.

[35] D. Balfanz, G. Durfee, D. K. Smetters, and R. E. Grinter, "In search of usable security: Five lessons from the field," *Security & Privacy, IEEE*, vol. 2, no. 5, pp. 19–24, 2004.

[36] S. Chiasson, R. Biddle, and A. Somayaji, "Even experts deserve usable security: Design guidelines for security management systems," in *Symposium on Usable Security and Privacy (SOUPS) Workshop at Usable IT Security Management (USM)*, 2007, pp. 1–4.

[37] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Trustworthy and effective communication of cybersecurity risks: A review," in *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST) at 5th International Conference on Network and System Security (NSS)*, 2011, (In press).

[38] A. Josang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security usability principles for vulnerability analysis and risk assessment," in *23rd Annual Computer Security Applications Conference (ACSAC'07)*. IEEE, 2007, pp. 269–278.

[39] A. Dix, J. Finlay, G. D. Abowd, and R. Beale, *Human-Computer Interaction*, 3rd ed. Prentice hall, 2004.

[40] P. Jaferian, D. Botta, F. Raja, K. Hawkey, and K. Beznosov, "Guidelines for designing IT security management tools," in *2nd ACM Symposium on Computer Human interaction For Management of information Technology*, 2008, pp. 1–10.

[41] P. Jaferian, K. Hawkey, A. Sotirakopoulos, and K. Beznosov, "Heuristics for evaluating it security management tools," in *2011 Annual Conference Extended Abstracts on Human factors in Computing Systems*. ACM, 2011, pp. 1633–1638.

[42] U.S. Department of Health & Human Services (HHS), "Research-based web design & usability guidelines," 2006. [Online]. Available: http://www.usability.gov/guidelines/guidelines_book.pdf (ISBN 0-16-076270-7)