From Paternalistic to User-Centred Security: Putting Users First with Value-Sensitive Design

Steve Dodier-Lazaro
University College London
London, WC1E 6BT, UK
s.dodier-lazaro@cs.ucl.ac.uk

M. Angela Sasse
University College London
London, WC1E 6BT, UK
a.sasse@ucl.ac.uk

Ruba Abu-Salma
University College London
London, WC1E 6BT, UK
r.abu-salma@cs.ucl.ac.uk

Ingolf Becker
University College London
London, WC1E 6BT, UK
i.becker@cs.ucl.ac.uk

Abstract

Usable security research to date has focused on making users more secure, by identifying and addressing usability issues that lead users to making mistakes, or by persuading users to pay attention to security and make secure choices. However, security goals were set by security experts, who were unaware that users often have other priorities and value security differently. In this paper, we present examples of circumventions and non-adoption of secure systems designed under this paternalistic mindset. We argue that security experts need to identify user values and deliver on them. To do that, we need a methodological framework that can conceptualise values and identify those that impact user engagement with security. We show that *(a)* engagement with, and adherence to security, are mediated by user values, and that *(b)* it is necessary to model those values to understand the nature of security's failures and to design viable alternatives.

Author Keywords

Value-Sensitive Design; Security; Productive Security; Research Methods

ACM Classification Keywords

H.5.2 [User Interfaces]: User-centered design; K.4.3 [Organizational Impacts]: Computer-supported collaborative work

Introduction

The usable security research community, in its investigations of how users interact with security mechanisms, has often found security to hinder or compete with user goals, sometimes because of unusable user interfaces [7, 12, 16]. This has led some to believe in the existence of a trade-off between usability and security. In some cases, however, users choose to disengage from security altogether. Concepts like productivity [3, 24], cost [14] or utility [22] have come up in the field's literature, which could explain why.

The usable security community has so far focused on enhancing the usability of already existing security systems, with a narrow interpretation of usability: they focus exclusively on 'fixing' human users (rather than fixing technologies), so as to render them 'able' to 'use' security. Consequently, non-usability-related causes of user disengagement from security are not examined. Security experts fail to notice the divergence between what they imagine user values to be and users' actual values. This divergence, in turn, can cause otherwise usable security artefacts to be useless, counter-productive or even harmful.

Examples abound, e.g. in the literature on security warnings. Usable security researchers aim to 'fix' user compliance to warnings, e.g. by making them waste time re-typing some of the warning's content [6] or by showing different warnings every time to prevent them from recognising warnings [2]. They propose such approaches even though warnings sometimes provide no security benefit at all [14]. Sasse [21] argued that instead, the community should acknowledge that users have other priorities, and focus on *how often* warnings must be shown.

Similar issues exist with password research. Bonneau et al. argue in favour of training users to remember 15-character random passwords [5]. Yet, the fact it *can* be achieved in a lab doesn't mean it is something users would want to do: entry times and error rates increase dramatically with $8+$-character passwords [23], and longer passwords are more likely to fail after periods of non-usage (e.g. vacations). In the real world, users' main concerns are 'Will I be able to remember it?', and 'Will I be able to enter it correctly?'. 'How secure is it?' comes a very distant third.

We argue that Value-Sensitive Design (VSD) can help our research community understand what users value, and realise it has been working against users' interests by adopting a narrow stance on the goals of usable security. Too little focus has been put on what users' priorities are – and how to get there securely. In this paper, we reflect on past research experiences which taught us that (a) engagement with security is mediated by user values and (b) those values must be modelled if we want to understand the nature of security failures and to design viable alternatives. We discuss how relevant user values are to user adoption and usage of security technologies, and discuss the potential benefits of embracing VSD for our community.

Case Studies in Personal Computing

Why Secure Communication Tools Don't Get Adopted

Usability has long been considered a key challenge for secure communications, in particular encryption. Several users studies (e.g. [9, 13, 26]) have examined why users fail to use existing secure communication tools such as PGP correctly, often concluding that significant security failures arise due to user interface design flaws. Abu-Salma et al. [1] interviewed 60 users about their experience with different communication tools and their perceptions of the tools' security and privacy. Despite visible usability issues in some tools' interfaces, participants did not report usability to be a primary obstacle to their adopting of secure tools. Instead, they were concerned about the fragmentation of

user bases across incompatible tools. Most communications are spontaneous rather than planned; to reach their communication partners, users either need to use the same communication tool, or tools need to be interoperable. As users valued the convenience of using the most directly available communication tool more than they valued security, they did not adopt secure communication tools. By developing completely new tools, the security community has failed to satisfy users' primary expectation: reaching their peers as conveniently as possible.

A Value-Sensitive Analysis of Application Appropriation
Dodier-Lazaro et al. [11] interviewed 13 Linux users about how they adopt and abandon apps, and how they adapt them with plugins. Using a value-sensitive analysis, they found that app adoption was primarily driven by utility (the presence of specific features or content); app abandonment by utility and reliability (the app was not slow, unstable or too heavy); and the adoption of app plugins by productivity (helping users perform tasks or access resources quicker) and utility. Security played a minor role in participants' app appropriation decisions, behind all the aforementioned values. This work was motivated by the fact that app developers on platforms where sandboxing is available often refuse to support it. They fear losing users because of the restrictions sandboxing imposes on features and app plugins. The study confirmed the legitimacy of those fears, and calls into question why sandboxes are so disruptive to utility, the main driver of app adoption and retainment.

Case Study in Organisational Security

Bartsch and Sasse [3] analysed interviews with 118 employees of a trans-national company on their compliance to access control measures in diverse contexts. Issues were found in the procedures for policy changing and in the decision-making process of policies, which affected employees' productivity and caused them to circumvent security in order to remain productive. In that organisation, a value conflict between security and productivity existed. Still, employees reported discomfort in breaching security policies, and some even went on to deploy their own security measures, showing they valued security.

Bartsch et al. point out the role of social values: some employees would grant access to systems so that requesting employees would escape the emotional cost of being denied access; or, they would grant another team access to a system as a bargaining chip for future relations. The employees who deployed their own security measures relented the absence of high-level security guidelines from the organisation: they valued its expertise on security, despite rejecting how security was implemented. While those value conflicts were less commonly witnessed than the security-productivity conflict, their existence warrants a deeper investigation of how social values can supersede security.

Organisations' information systems are used and maintained by humans with diverse interests and hierarchical structures. The values embedded in those interests and structures mediate how they cooperatively maintain information systems, including security components. Hence, the values of an organisation must be taken into account when designing and deploying security measures for its systems.

A General Problem in Usable Security

We have provided examples that demonstrated that that what users value – utility, productivity, ease of use, etc. – causes them to disengage from secure systems that reduce utility and usability. But are these studies an exception to how security fits within users' experiences? Or is security more often at odds with user values than was previously assumed? We argue value conflicts are commonplace in

the use of security technologies, albeit little attention has been devoted to them. Due to their nature, some categories of security systems are likely to be concerned.

For instance, if users did pay attention to passive security notifications like phishing bars, their productivity would drastically decrease – in return for negilible security benefits [14]. Their lack of attention could be explained by habituation effects or insufficient visual cues, but also by a value conflict with productivity. While designs that prevent habituation and provide more salient visual cues could solve the former two issues, the existence of a value conflict entails that passive notifications are fundamentally inadapted.

Authentication systems are too influenced by a multitude of values. Productivity is a reason why users bypass authentication systems altogether [15, 24]. Users also share authentication credentials as a form of trust signalling [18, 19], or to avoid excessive delays in authorising newcomers [3]. Some users do not trust providers of password managers and want to ensure they can always access their passwords [8]. Reputation matters too: users may refuse to perform security actions to avoid embarassment should they fail to use the mechanism [4, 10].

Dealing with Users' Misconceptions about Security
One difficulty of security design is that users often struggle to understand whether computer systems they use provide security. Users rely on incorrect heuristics to determine if a system is secure [8, 17], and on misconceptions on the nature of threats they face [20, 25].

As such, users' conception of a 'security' value differs from the 'security' value that is imagined by the security engineers who design security technologies. Ultimately, how the presence of 'security' is perceived by users is irrelevant to the actual presence of security. Users may perceive a system to be 'secure' when it isn't, or to be 'insecure' when it is. This implies that security designers must design for security, but also for visual and interactional cues that signal the 'security' value of their target users. Likewise, empirical and technical analyses must distinguish security from user 'security' in order to be accurate.

VSD can Help Security Research

We have seen that value conflicts exist across multiple topics covered in usable security research, both for personal and organisational computing. Let us now discuss the benefits of investigating these value conflicts.

Firstly, VSD forces security researchers to systematically document users' behaviour drivers. As we analyse more systems with VSD, patterns of value conflicts might emerge for families of security mechanisms, or for specific user populations. For instance, all forms of delegated authentication might conflict with privacy-oriented users. Workers who frequently hire interns might always attempt to bypass centralised access control systems, etc. Knowing that such patterns exist enables service providers to propose only forms of security that will not conflict with user expectations. It may help researchers identify which types of technologies are likely to be unsuitable beyond repair, and which ones are candidates for re-designing.

Secondly, fully designing, evaluating and deploying a security artefact is costly. If security designers had the ability to anticipate an artefact's failure in the wild, they could spare expenses by eliminating this artefact early in the design cycle. Since value conflicts cause disengagement from security, Value-Sensitive conceptual and empirical analyses of targeted use contexts are perfectly adequate tools to provide such design requirements.

Finally, VSD could be the tool we have been missing to address security non-compliance. Methods of investigation that solely observe lab interactions can only identify why users fail to use a security mechanism, and only improve task performance when users are already acceptant of the security mechanism's benefits. A security mechanism that is more usable, but equally undesirable than currently deployed ones will still be rejected by disengaged users. Therefore, identifying the root causes of disengagement can only be done by studying users' rationales for *not* using as security mechanism, not by studying how they, or others, fail to use it when they *already want to*.

Conclusion

We have provided examples of how the current narrow focus on experts' values when designing security leads to circumventions of security mechanisms and non-adoption of secure solutions. Arguably, it also has done lasting damage to the trust users have in what security experts tell them. Usable security experts continue to disregard the preferences and priorities of users, the economic implications of deploying non-user-centred security, and the disconnect between how security is valued by security experts and valued by users. This lack of attention to users' values has led to unusable, ineffective and *unused* security mechanisms.

We propose to broaden our perspective on the goals of usable security research, by putting user values at the center, and by making the protection against threats that expert agree upon a secondary goal. Indeed, there cannot be security without user adhesion. Mechanisms that are inefficient or useless stand no chance of actually improving security out there in the wild. Security mechanisms must respect what users value, be it productivity, cost, credibility, etc. Embracing user values and designing value-sensitive security mechanisms is the way towards security that is adopted by users, and that actually works. The current paradigm of usable security, leading to mechanisms which not only users reject, but which also wastes effort and resources for dubious security benefits, is no longer viable.

References

[1] Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. 2017. Obstacles to the Adoption of Secure Communication Tools. In *Security and Privacy (SP), 2017 IEEE Symposium on (SP '17)*. IEEE Computer Society.

[2] Bonnie Brinton Anderson, C. Brock Kirwan, Jeffrey L. Jenkins, David Eargle, Seth Howard, and Anthony Vance. 2015. How Polymorphic Warnings Reduce Habituation in the Brain: Insights from an fMRI Study. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2883–2892. DOI: http://dx.doi.org/10.1145/2702123.2702322

[3] Steffen Bartsch and M. Angela Sasse. 2013. How Users Bypass Access Control and Why: The Impact of Authorization Problems on Individuals and the Organization. In *Proceedings of the 21st European Conference on Information Systems (ECIS 2013)*. 53. http://aisel.aisnet.org/ecis2013_cr/53/

[4] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 workshop on New security paradigms (NSPW '08)*. ACM, New York, NY, USA, 47–58. DOI: http://dx.doi.org/10.1145/1595676.1595684

[5] Joseph Bonneau and Stuart Schechter. 2014. Towards reliable storage of 56-bit secrets in human memory. In *Proc. USENIX Security*.

[6] Cristian Bravo-Lillo, Lorrie Cranor, Saranga Komanduri, and Stuart Schechter. 2014. Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It$\vphantom{}$. In *Symposium On Usable Privacy and Security*. USENIX.

[7] Sacha Brostoff and M. Angela Sasse. 2000. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *People and Computers XIV âĂŤ Usability or Else!: Proceedings of HCI 2000*, Sharon McDonald, Yvonne Waern, and Gilbert Cockton (Eds.). Springer London, London, 405–424. http://dx.doi.org/10.1007/978-1-4471-0515-2_27

[8] Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06)*. USENIX Association, Berkeley, CA, USA. http://dl.acm.org/citation.cfm?id=1267336.1267337

[9] Sandy Clark, Travis Goodspeed, Perry Metzger, Zachary Wasserman, Kevin Xu, and Matt Blaze. 2011. Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System. In *USENIX Security Symposium*. 8–12.

[10] Robert Coles, Jonathan Griffin, Hilary Johnson, Brian Monahan, Simon E Parkin, David Pym, M Angela Sasse, and Aad van Moorsel. 2008. Trust economics feasibility study. In *DSN 2008 Workshop on Resilience Assessment and Dependability Benchmarking*. IEEE Computer Society 2008, Anchorage, Alaska, USA.

[11] Steve Dodier-Lazaro, Ingolf Becker, Jens Krinke, and M. Angela Sasse. 2017. *No Good Reason to Remove Features: Expert Users Value Useful Apps over Secure Ones*. Research Notes. University College London. http://www.cs.ucl.ac.uk/research/research_notes/

[12] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 2893–2902. DOI: http://dx.doi.org/10.1145/2702123.2702442

[13] Simson L Garfinkel and Robert C Miller. 2005. Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express. In *ACM Proceedings of the Symposium on Usable Privacy and Security*. 13–24.

[14] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop (NSPW '09)*. ACM, New York, NY, USA, 133–144. DOI: http://dx.doi.org/10.1145/1719030.1719050

[15] Philip G. Inglesant and M. Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. ACM, New York, NY, USA, 383–392. DOI: http://dx.doi.org/10.1145/1753326.1753384

[16] Clare-Marie Karat, John Karat, Carolyn Brodie, and Jinjuan Feng. 2006. Evaluating interfaces for privacy policy rule authoring. In *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI '06)*. ACM, New York, NY, USA, 83–92. DOI: http://dx.doi.org/10.1145/1124772.1124787

[17] I. Kirlappos and M. A. Sasse. 2012. Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security Privacy* 10, 2 (March 2012), 24–32. DOI: http://dx.doi.org/10.1109/MSP.2011.179

[18] Iacovos Kirlappos and M Angela Sasse. 2015. Fixing Security Together: Leveraging trust relationships to improve security in organizations. In *USEC*.

[19] Niels Raabjerg Mathiasen and Susanne BÃÿdker. 2011. Experiencing security in interaction design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 2325–2334. DOI: http://dx.doi.org/10.1145/1978942.1979283

[20] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. ACM, New York, NY, USA, 6:1–6:17. DOI: http://dx.doi.org/10.1145/2335356.2335364

[21] A. Sasse. 2015. Scaring and Bullying People into Security Won't Work. *IEEE Security Privacy* 13, 3 (May 2015), 80–83. DOI: http://dx.doi.org/10.1109/MSP.2015.65

[22] D. K. Smetters and R. E. Grinter. 2002. Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 workshop on New security paradigms (NSPW '02)*. ACM, New York, NY, USA, 82–89. DOI: http://dx.doi.org/10.1145/844102.844117

[23] Brian C. Stanton and Kristen K. Greene. 2014. *Character Strings, Memory and Passwords: What a Recall Study Can Tell Us*. Springer International Publishing, Cham, 195–206. DOI: http://dx.doi.org/10.1007/978-3-319-07620-1_18

[24] Dennis D Strouble, G Schechtman, and Alan S Alsop. 2009. Productivity and usability effects of using a two-factor security system. *Proceedings of SAIS* (2009), 196–201.

[25] Rickm Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*. ACM, New York, NY, USA, 11:1–11:16. DOI: http://dx.doi.org/10.1145/1837110.1837125

[26] Alma Whitten and J. Doug Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*.