Journal of Information Security and Applications 34 (2017) 76–81

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Contemplating human-centred security & privacy research: Suggesting future directions

Karen Renaud[a], Stephen Flowerday[b]

[a] University of Glasgow, United Kingdom
[b] University of Fort Hare, South Africa

ARTICLE INFO

Article history:

ABSTRACT

This position paper is a reflective look at the state of Human-Centred Security & Privacy (HCSP) research and the paradigms that have informed and driven the research. It is important to reflect and examine, because, as Harrison et al. [1] argue, with respect to HCI, "*the lack of clarity about the epistemological distinctions between paradigms is a limiting factor in the development of the field*" (p. 1). We discuss the current state of play and then suggest possible explanations and suggestions for the way forward for our research field. This paper aims to prompt a discussion of the directions HCSP should take, and ways we could deploy to encourage maturation of the field.

1. Introduction

The field of *Usable Security* emerged at the beginning of the 21st century, launched in 1999 by the seminal paper by Adams and Sasse [2], which pointed out that end-users were not the enemy. Before this, the end-user was somewhat derided for his/her poor password choices and non-compliance with good password practice. Their paper was one of the first to suggest that the usability of security technologies and tools deserved serious attention.

The new branch of human-computer interaction (HCI) focusing on security thus came into being. It soon embraced privacy as well. The emerging field of what we will call "*Human-Centred Security & Privacy*" (HCSP) has since become established, reflecting the acknowledgment of the crucial role the end-user plays in securing information and systems. Today, in 2016, a number of workshops and conferences specifically call for human-centred security and privacy related papers (See Appendix).

In order to predict how the HCSP research field might, and ought to, mature, we will first examine the development of its parent field: HCI. We then compare the progression of HCSP with HCI, and suggest explanations for the current focus of HCSP research. We conclude by suggesting how the field ought to develop in order to ensure that we make the same impact HCI has made on people's everyday lives.

2. Human computer interaction

Myers [3] argues that the HCI field was launched in 1960 with the development of direct manipulation of graphical objects. Carroll [4] pins the birth of HCI, with an end-user rather than hardware focus, to the 1970s. The original focus, he argues, was pure *usability*. Carroll says the initial HCI stalwarts appeared to be propagating a heretical view, and had to fight to establish HCI as a serious research area. Now, Carroll says, "*HCI is a vast and multifaceted community, bound by the evolving concept of usability, and the integrating commitment to value human activity and experience as the primary driver in technology.*"

Whereas Carroll and Myers chart the development of HCI in small steps Bødker [5] takes a broader view, referring to HCI's progress as a succession of *waves*.

The **first** wave, she explains, focused on the individual. The individual's perceptions, cognition and behaviours were tested and modeled.

The **second** wave moved from studying the individual to contemplating social behaviours, agency and interactions within workplaces and with others via technology. The focus moved to groups working with applications. Instead of studying the human, the researchers now studied work settings. Context and situational analysis came to the fore.

The **third** wave then broadened the focus even further to incorporate studies of the integration of technology into people's everyday lives. Now researchers started to talk about user experience and meaning making. Technology becomes the extension of the individual, with the boundaries between the individual and

E-mail addresses: cyber4humans@gmail.com (K. Renaud), sflowerday@ufh.ac.za (S. Flowerday).

http://dx.doi.org/10.1016/j.jisa.2017.05.006
2214-2126/© 2017 Published by Elsevier Ltd.

the technology blurring. The third wave coincided with the diffusion of mobile devices, and the vastly increased functionality in the hands of every person. Social networking sites also entered the fray and offered a whole new area for research. Researchers, during this wave, started to make the point that it was necessary to study technology use *in the wild* [6]. Korn and Bødker [7] argue caution in terms of testing in the wild; saying that technology should not merely be dumped on people. They urge the combination of participatory prototyping, experiments and in-the-wild studies.

Harrison et al. [1] takes a similarly high level look at HCI, and proposes three different paradigms, the first being engineering research. This was characterised by the design of cockpits to reduce pilot errors, for example. Harrison et al. argue that the next paradigm was the cognitive revolution. They argue that this paradigm was dominated by the idea of humans as information processing units. The third paradigm, they explain, came from the realisation that the information-processing paradigm did not match all cases. The new paradigm embraced the construction of meaning, as it occurs while people interact with technology. It also incorporated the realisation that people's understanding and behaviour is informed and influenced by their context, their physical and social situations. They also refer to the need to study humans creating meaning from multiple perspectives and for design to be focused primarily on values.

In 2015 Bødker returned to her wave theme 10 years after her original keynote [8]. She reviewed progress over the last 10 years and says that the challenge is to *"go beyond embracing individual experience as it develops over time when people carry out activities and use artifacts"*. She holds back from predicting the arrival of a fourth wave, concluding that HCI is somewhat chaotic at present with a mishmash of technologies, use situations, methods, and concepts characterising current research in the field [8].

Bødker [8] argues for the fact that the making and sharing of meaning is essential. She laments the fact that much research does not make it clear how it benefits people, or impacts their lives, or, indeed, what the meaning of the research is to the man and woman in the street. The lesson to be taken from Bødker is that a field has to mature to achieve its full potential.

HCSP seems to have less of a challenge in demonstrating the impact of their research, since improvement in individual security is obviously a desirable outcome. We propose to take a meta view and to consider how to ensure that this happens.

3. Examining HCI research

In order to determine whether the papers published in the HCI field reflect these waves, we took three snapshots of the CHI conference (Human Factors in Computing Systems), the top HCI conference, for three years: 2004, 2010 and 2016. We did not snapshot all the interim years since Bødker [5] gave her keynote. Since CHI is an established and mature conference we expected to see changes manifesting over longer periods of time than for younger conferences which have not yet stabilised.

A qualitative judgement was made based on the titles of the conference papers and then we classified and quantified the papers based on our understanding of the three waves before generating the graphics. A total of 1600 titles were analysed. It is thus possible that a detailed perusal of the papers could have led to a different classification but, since the title is meant to encapsulate and describe the content, it seemed to be a reasonable signal to judge the paper's focus. We categorised the papers as belonging to one of the three 'paradigms' or 'waves' as follows:

First Wave: The focus of the paper was the *individual*, as participant, agent or unwitting actor.

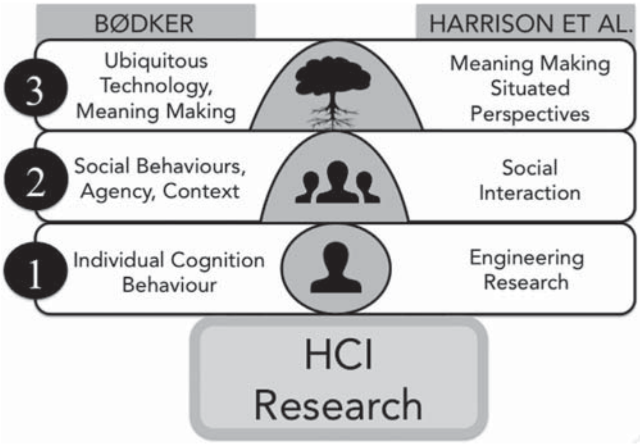
BØDKER
HARRISON ET AL.
3
Ubiquitous Technology, Meaning Making
Meaning Making Situated Perspectives
2
Social Behaviours, Agency, Context
Social Interaction
1
Individual Cognition Behaviour
Engineering Research
HCI Research

Fig. 1. HCI Waves of Maturity.

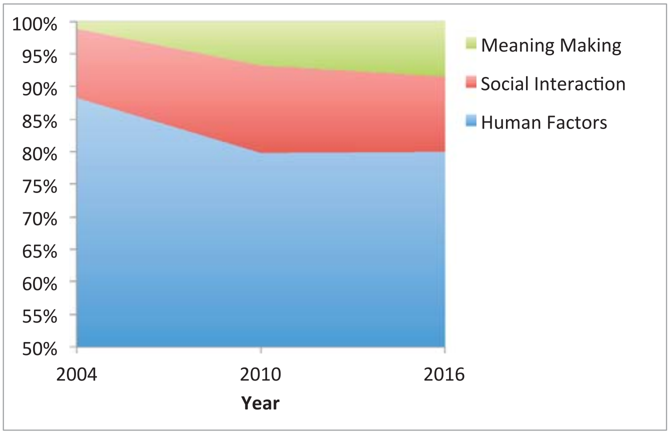

Fig. 2. CHI Papers over three years (Note that Y axis starts at 50%).

Second Wave: The focus here was on the *social context*: software that facilitates and supports collaboration and interaction. The distinction here was that the focus is on the software that enables collaboration, not on the individual's use thereof. In this category we included studies of participative design, and studies of the use of technology within a particular context or culture. It should be noted that the study's focus should not be on the individual user as agent, but rather on the context and social aspects of the situation.

Third Wave: What distinguishes this wave are two types of focus. The first is ubiquitous computing, and how people integrate various devices and technologies into their lives. The focus has moved on examining and revealing to the *meaning* of the interaction. Other studies that try to make meaning are included here. Examples are studies that take a meta view of a particular aspect, or studies that analyse a number of research studies and extract principles for design.

The graph in Fig. 2 certainly appears to confirm the emergence of the waves Harrison et al. [1] and Bødker [8] refer to.

4. Human-centred security & privacy

At present, the field of human-centred security & privacy (HCSP) is much younger than HCI. We took a snapshot of the research in the area by classifying all the papers accepted by the SOUPS conference (Symposium On Usable Privacy and Security) from 2012 to 2016. The choice of SOUPS was motivated by the fact that it was the first conference dedicated solely to this area.

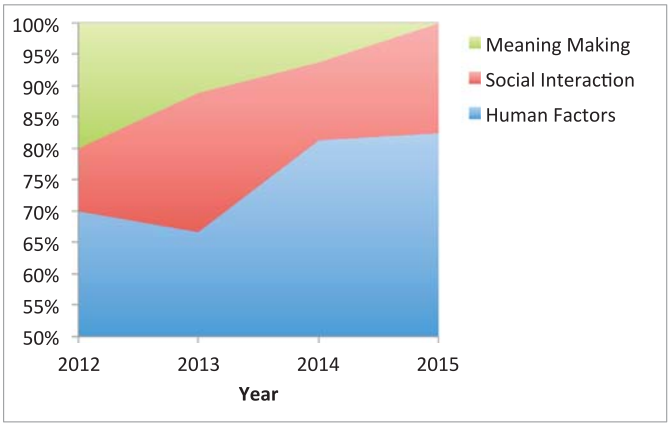

Fig. 3. SOUPS papers ranked in terms of Waves (Note that Y axis starts at 50%).

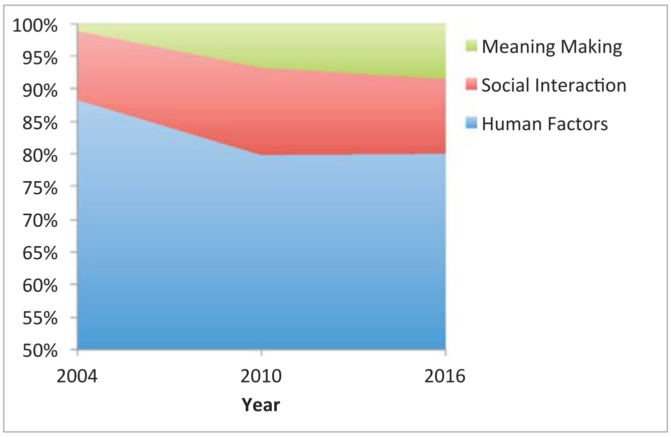

Fig. 4. ICIS papers ranked in terms of Waves (Note that Y axis starts at 50%).

A number of other dedicated conferences/workshops were established subsequently, such as STAST, USEC and EuroUSEC, while other HCI conferences also publish these papers they do so in addition to regular HCI papers; for these conferences HCSP is still a subgroup of the bigger HCI field. Finally, in a number of online rankings (see Appendix) the SOUPS symposium is ranked higher than these other workshops/symposiums.

Figure 3 shows the wave ratio of SOUPS papers, over the last five years, in terms of Bødker's first, second and third waves. It should be noted that papers classified as "Social" were generally about interpersonal or organisational behaviours and participatory design. (Papers talking about individuals interacting with social networking sites were classified as human-factors research). Papers classified in terms of the third wave were those that mentioned context or situational impact, or meaning making. For example, "*Improving Older Adults' Online Security: An Exercise in Participatory Design*" [9] was classified as a second wave paper, since it addressed participatory design. We classified "*Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations*" [10] as a third wave paper because it embraced the concept of meaning making.

It is clear from this graph that the field is still focusing very strongly on the individual's perspective of security and privacy. There is some evidence of the emergence of the second and third waves, but they do not seem to be gaining traction. In fact, their share of the pot seems to be diminishing in favour of even more human-factors papers.

It must be considered that this graph might not accurately reflect the state of the HCSP research field. It could be that people working in the second wave are not publishing at SOUPS or that SOUPS attracts primarily individual-focused papers. We thus identified the top Information Systems conference that also published HCSP papers to see whether second wave papers were being diverted there. We identified ICIS as being one of the top conferences and classified the papers published in the last 4 years (2016 papers were not available). We also categorised papers published at the Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13 since this workshop is focused on ground-breaking information systems HCSP research, and many of their papers subsequently appear in top-ranking journals.

Figure 4 (ICIS papers) demonstrates a different spread from SOUPS. Fig. 5 (Dewald Roode workshop) demonstrates a stronger third-wave presence than the other conferences.

To end off this section we mention a few papers to provide examples of the kinds of research that has recently appeared in each of the three waves.

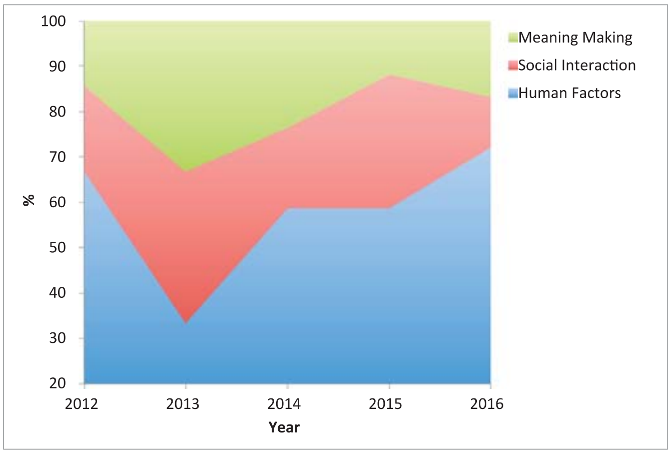

Fig. 5. Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13 papers ranked in terms of Waves (Note that Y axis starts at 20%).

4.1. First wave: Human factors

A number of recent papers address the issues users have with security aspects of their devices and systems. For example: "*Ask Me Again But Don't Annoy Me: Evaluating Re-authentication Strategies for Smartphones*" [11] and "*They Keep Coming Back Like Zombies*": *Improving Software Updating Interfaces*" [12]. There are also papers about user motivations to comply, or to behave securely "*Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice*" [13], or to communicate new insights into human-related security behaviours "*Snooping on Mobile Phones: Prevalence and Trends*" [14] and "*Understanding Password Choices: How Frequently Entered Passwords are Re-used Across Websites*" [15]

4.2. Second wave: Social & work context

Papers in this category focus on organisational security, or participatory design. For example: "*Synchronised smart phones: The collision of personal privacy and organisational data security*" [16], "*Improving Older Adults' Online Security: An Exercise in Participatory Design*" [9] and "*Top management can lower resistance toward information security compliance*" [17].

4.3. Third Wave: UX & Making Meaning

Bødker [8] says that research in this wave is characterised by meaning making. "*Visible handling of the many emergent forms of* *devices is one element of this that needs more exploration, and the visibility of meaning and meaning-making an equally important one.*" A good example of this kind of paper is the paper titled "*Passwords and the Evolution of Imperfect Authentication*" by Bonneau et al. [18] that enters the password fray. For years now researchers have been trying to persuade or compel people to choose better passwords. Bonneau and co-authors write an excellent treatise, making the argument that we ought to stop focusing on the end user, and rather find other ways to bolster security. Some other examples of papers that attempt to do this in the conferences we reviewed are: [19–25].

5. Explanations for HCSP first wave focus

A number of explanations for the current HCSP first-wave focus suggest themselves. The first is that HCSP is a much younger field than HCI and it could be that a certain critical mass of papers is required in order fully to understand the human factor aspects of humans interacting with security and privacy technologies.

Gregor and Hevner [26] characterise the maturity of design science research on two dimensions: application domain maturity and solution maturity. Research that is low on both these dimensions is focused on invention, focusing on new problems and new solutions. As the field matures in both dimensions the problems are revealed and become well understood. Moreover the range of solutions are established and researchers choose which to apply rather than coming up with new problems or solutions. Since there are a number of similarities between design science and HCSP research, this argument might support the explanation we advanced in the previous paragraph.

Further to the previous point, is the fact that the field, as a whole, now knows how to carry out empirical experiments to test human factors aspects. We have established a benchmark for these. So, if people want to get their research published they follow the guidelines, carry out and publish the research. New wave research is not as well delineated and might be more likely to be rejected by reviewers. It is certainly comforting to keep doing the same kinds of research, but research fields need to mature to ensure they keep advancing and make a real impact.

Another explanation could be that in security accountability is a strong driver. Mostly this is because it has to be possible to prove, beyond reasonable doubt, that person A did carry out a particular action. That is why passwords have to be kept secret. If person A can prove that an unknown person B could have got hold of their password without their knowledge, doubt is introduced. Accountability can no longer be proven.

According to Hevner et al. (2004) [27] the two basic information systems research paradigms are behavioural research, which focuses on what is true and design research which deals with utility. They posit that truth and utility are inseparable; that truth informs design and that utility informs theory. Being conscious of this view we argue that security is a given and we acknowledge that it is essential not to weaken security protocols. Equally, we argue that individuals do not necessarily need to be consciously aware of the security functions taking place while they embrace technology. In many cases security system designers have not embraced this insight.

There is also the possibility that we ought not to have compared HCSP to HCI because the fields are more different than they are similar. Security-related interactions might well be profoundly different from HCI, and more comparable to some other research field. However, given the fact that HCSP papers are generally published in a named stream of major HCI conferences, it did seem that the comparison would provide the insights we were looking for.

6. Where to from here?

When researchers in a research field are used to applying one particular paradigm some kind of event needs to disrupt thinking to prompt a switch to a new paradigm. When this happens the research starts to change, the published papers start to demonstrate increasing maturity and the research starts to make a difference to real people's lives. We cannot really claim that HCSP has achieved this maturity, as yet. Most of the security products being used by John and Jane Citizen are still not usable enough, and most of the industry relies primarily on awareness-raising endeavours in order to improve their employees' resilience to cyber attack. Yet each year the number of successful hacking attacks increases so there is little evidence that awareness raising, as currently implemented, is particularly effective. It is time for some reflection.

Other fields have been disrupted by external or unexpected events. The medical field was disrupted when antibiotics were discovered. Criminal forensics was revolutionised by discovery of fingerprints as an identifier, and again when DNA testing became feasible.

The disruptions that caused the step changes in HCI were technological: (1) collaborative software, and (2) mobile devices. Can we draw parallels to similar disruptions that might cause HCSP to step-change? The first HCI step change forced researchers to start broadening their focus to include the social element of human computer interaction, rather than merely the human and their device. Security, unlike interaction, tends to be a solo activity. It is certainly worth considering how we could create communities within organisations to help each other out with their information security needs. The next step change in HCI happened with the move from desktop (fixed) to mobile devices. It opened a whole new arena for interaction research. A number of technological developments have emerged with interesting challenges in terms of HCSP research. Examples include the Internet of Things [28–30], e-health [31], big data [32], cloud technology [33] and robotics [34]. Don and Alex Tapscott [35] argue that the biggest technological disruption in the next few years will be blockchain. There is much to be done to help improve the general understanding of this technology if these authors' predictions come to fruition [36].

What kind of event would disrupt HCSP research and encourage it to embrace new paradigms, to start maturing? It is clear that many HCSP researchers are already working in the areas prompted by technological improvement, but the focus is still primarily on the individual. Because technological improvements have not really disrupted HCSP research, the disruption might have to come from reconsidering the methods and methodologies we deploy in our research instead.

A column published by Ujwal Arkalgud [37] offers some valuable insights. He argues that his research field (marketing) needs to be disrupted because the limitations in their current methods are becoming clear. There is some similarity between his field and HCSP because we tend to use the same tools they do. He argues that "*traditional research methods like focus groups, polls and surveys struggle to deliver the accuracy, clarity and actionability that organizations require*". He says that effective research needs to be observational, belief-driven and scalable. Let us take a moment to consider whether his arguments apply equally well to HCSP research.

Observational: We could stop asking people about their security behaviour and rather observe what they do. We know people are not necessarily frank and open about their security behaviours, and this leads to responses informed by social desirability instead of reality. Moreover, surveys measure intention, and not actual behaviour, and the two are weakly correlated. We ought therefore not to place so much faith in survey results and find ways to carry out ethical observation studies.

Scalable: We could stop drawing conclusions from studies carried out with only 100s of participants, and we ought to stop segmenting people based on age, expertise or education. Cyber security is a problem for all sectors of society and hackers certainly don't segment people this way when they decide to attack them.

Belief-Driven: Arkalgud argues that *"understanding people's underlying beliefs is the path to uncovering their real motivations"*. Back in 1999 Adams and Sasse [2] shone the light on the divide between information security professionals and end users. Almost two decades have passed and that divide has not yet been bridged. Those who secure systems still fail to understand why users behave the way they do. This category of disruption asks us to start listening to our end users, and to stop telling them what to do without considering their perspectives.

Salvo [38] points out that innovation is never a solo mission. Certainly if we want to move towards Arkalgud's vision of more impactful research we cannot do this alone. Salvo says "*Whenever and wherever we reduce the friction between our connections, our overall productivity tends to soar upward*". The academic environment is intensely competitive, yet researchers achieve so much more when they collaborate than when they attempt to work alone. We conclude this section by urging researchers in this field to work with others to move our field towards maturity. Only by working together can we make the impact on everyday security we all want to make.

7. Limitations

We carried out this study to take a broad-brush approach in terms of contemplating the HCSP field of research. We chose the top HCI conference (CHI) and the top HCSP and two of the top Information Systems conferences (SOUPS, ICIS and the Dewald Roode Workshop). A different set of conferences, and choice of years, may have led to different profiles. Yet the profiles we did uncover are interesting. They act as a marker, a signal for us to consider our field more carefully.

We, the two authors, independently assigned the papers to one of the three waves, and agreed on the final classification. While having two authors classify papers removes a certain measure of subjectivity, it has to be acknowledged that we cannot rule it out altogether.

8. Conclusion

This paper conducted a meta review of the research being undertaken in HCSP. We contemplated the maturity of the field, using the waves proposed by Bødker and Harrison et al.. We showed how the major HCSP conferences' papers appeared to demonstrate that we were still working in the first wave. A look at some information systems conferences showed that second and third-wave papers were starting to appear. We advanced some explanations for this, and make some suggestions for a way forward, to ensure that our field does mature and improve the security of computer users. We penned this paper to open a discourse in the research community. We would like to hear from other researchers on this topic.

Acknowledgements

We thank Melanie Volkamer for helping to compile the list of conferences in the Appendix.

Appendix. A non-exhasutive list of HCSP conferences

Purely HCSP

EuroUSEC	European Workshop on Usable Security
HAISA	International Symposium on Human Aspects of Information Security & Assurance
SOUPS	Symposium On Usable Privacy and Security
STAST	Workshop on Socio-Technical Aspects in Security and Trust
USEC	Usable Security
IFIP	Dewald Roode Workshop on Information Systems Security Research, IFIP WG8.11/WG11.13

HCSP as a subgroup

ACSAC	Annual Computer Security Applications Conference
CCS	ACM Conference on Computer and Communications Security
CHI	Conference on Human Factors in Computing Systems
ESORICS	European Symposium on Research in Computer Security
Euro S&P	IEEE European Symposium on Security and Privacy
FC	Financial Cryptography
HCI	British Human Computer Interaction
HCI International	Human Computer Interaction International
HICSS	Hawaii International Conference on System Sciences
IFIP Sec	IFIP Security
INTERACT	International Conference on Human-Computer Interaction
Mob HCI	Mobile Human Computer Interaction
NDSS	Network & Distributed System Security Symposium
NORDICHI	Norwegian Computer Human Interaction
NSPW	New Security Paradigms Workshop
OZCHI	Australian Computer Human Interaction
PETS	Privacy Enhancing Technologies Symposium
PST	Privacy Security and Trust
S&P	Security and Privacy
TRUST	Iinternational conference on Trust and Trustworthy Computing
UIST	ACM User Interface Conference and Technology Symposium
USENIX Security	The Advanced Computing Systems Association
WWW	World Wide Web

Conference rankings

A number of conference and journal rankings were consulted to identify the best conferences for sampling:

http://www.wi2.fau.de/_fileuploads/research/generic/ranking/information_technology.html
http://faculty.cs.tamu.edu/guofei/sec_conf_stat.htm
http://lipn.univ-paris13.fr/~bennani/CSRank.html
http://portal.core.edu.au/conf-ranks/?search=security&by=all&source=CORE2014&sort=arank
http://academic.research.microsoft.com/RankList?entitytype=3&topDomainID=2&subDomainID=12)

References

[1] Harrison S, Tatar D, Sengers P. The three paradigms of HCI. In: Alt. Chi. Session at the SIGCHI Conference on Human Factors in Computing Systems San Jose, California, USA; 2007. p. 1–18.

[2] Adams A, Sasse MA. Users are not the enemy. Communications of the ACM 1999;42(12):40–6.

[3] Myers BA. A brief history of human-computer interaction technology. interactions 1998;5(2):44–54.

[4] Carroll JM. Human computer interaction - brief intro. Encyclopedia of Human–Computer Interaction. Soegaard M, Dam RF, editors. Interaction Design Foundation; 2013.

[5] Bødker S. When second wave HCI meets third wave challenges. In: Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles. ACM; 2006. p. 1–8.

[6] Brown B, Reeves S, Sherwood S. Into the wild: challenges and opportunities for field trial methods. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM; 2011. p. 1657–66.

[7] Korn M, Bødker S. Looking ahead: how field trials can work in iterative and exploratory design of ubicomp systems. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. ACM; 2012. p. 21–30.

[8] Bødker S. Third-wave HCI, 10 years later—participation and sharing. interactions 2015;22(5):24–31.

[9] Munteanu C, Tennakoon C, Garner J, Goel A, Ho M, Shen C, et al. Improving older adults' online security: An exercise in participatory design Symposium on Usable Privacy and Security (SOUPS); 2015.

[10] Sundaramurthy SC, McHugh J, Ou X, Wesch M, Bardas AG, Rajagopalan SR. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016); 2016.

[11] Agarwal L, Khan H, Hengartner U. Ask me again but don't annoy me: Evaluating re-authentication strategies for smartphones. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016); 2016.

[12] Mathur A, Engel J, Sobti S, Chang V, Chetty M. " they keep coming back like zombies": Improving software updating interfaces. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016); 2016.

[13] Fagan M, Khan MMH. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016); 2016.

[14] Marques D, Muslukhov I, Guerreiro T, Carriço L, Beznosov K. Snooping on mobile phones: Prevalence and trends. Twelfth Symposium on Usable Privacy and Security (SOUPS 2016); 2016.

[15] Wash R, Rader E, Berman R, Wellmer Z. Understanding password choices: How frequently entered passwords are re-used across websites. Symposium on Usable Privacy and Security (SOUPS); 2016.

[16] Chigona W, Robertson B, Mimbi L. Synchronised smart phones: The collision of personal privacy and organisational data security.. South African Journal of Business Management 2012;43(2).

[17] Merhi M, Ahluwalia P. Top management can lower resistance toward information security compliance. ICIS; 2015.

[18] Bonneau J, Herley C, van Oorschot PC, Stajano F. Passwords and the evolution of imperfect authentication. Commun ACM 2015;58(7):78–87.

[19] De Luca A, Langheinrich M, Hussmann H. Towards understanding ATM security: a field study of real world ATM use. In: Proceedings of the sixth symposium on usable privacy and security. ACM; 2010. p. 16.

[20] Greig A, Renaud K, Flowerday S. An ethnographic study to assess the enactment of information security culture in a retail store. In: 2015 World Congress on Internet Security (WorldCIS). Dublin: IEEE; 2015. p. 61–6.

[21] Greitzer FL, Frincke DA. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In: Insider Threats in Cyber Security. Springer; 2010. p. 85–113.

[22] Seifert J, De Luca A, Rukzio E. Don't queue up!: user attitudes towards mobile interactions with public terminals. In: Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia. Ulm, Germany: ACM; 2012. p. 45.

[23] Tischer M, Durumeric Z, Foster S, Duan S, Mori A, Bursztein E, et al. Users really do plug in USB drives they find. In: IEEE Symposium on Security and Privacy. FAIRMONT, SAN JOSE, CA: IEEE; 2016. p. 306–19.

[24] Tyworth M, Giacobe NA, Mancuso V. Cyber situation awareness as distributed socio-cognitive work. SPIE Defense, Security, and Sensing. International Society for Optics and Photonics; 2012. 84080F.

[25] Yun H, Lee G, Kim D. A meta-analytic review of empirical research on online information privacy concerns: Antecedents, outcomes, and moderators. ICIS; 2014.

[26] Gregor S, Hevner AR. Positioning and presenting design science research for maximum impact.. MIS quarterly 2013;37(2):337–55.

[27] Hevner A, March ST, Park J, Ram S. Design science in information systems research. MIS quarterly 2004;28(1):75–105.

[28] Weber RH. Internet of things–new security and privacy challenges. Computer Law & Security Review 2010;26(1):23–30.

[29] Simon S. 'internet of things' hacking attack led to widespread outage of popular websites. 2016. October 22, http://www.npr.org/2016/10/22/498954197/internet-outage-update-internet-of-things-hacking-attack-led-to-outage-of-popula.

[30] Gallego J. Hacking light bulbs? new study exposes weaknesses in the internet of things. 2016. 5 November, http://futurism.com/hacking-light-bulbs-new-study-exposes-weaknesses-in-the-internet-of-things/.

[31] Kluge E-H W. Secure e-health: managing risks to patient health data. International journal of medical informatics 2007;76(5):402–6.

[32] Tene O, Polonetsky J. Privacy in the age of big data: a time for big decisions. Stanford Law Review Online 2012;64:63.

[33] Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1. IEEE; 2012. p. 647–51.

[34] Denning T, Matuszek C, Koscher K, Smith JR, Kohno T. A spotlight on security and privacy risks with future household robots: attacks and lessons. In: Proceedings of the 11th international conference on Ubiquitous computing. ACM; 2009. p. 105–14.

[35] Tapscott D, Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin; 2016.

[36] Swan M. Blockchain thinking: The brain as a dac (decentralized autonomous organization). In: Texas Bitcoin Conference; 2015. p. 27–9.

[37] Arkalgud U. Why the research industry is in desperate need of disruption. 2016. Oct 16, http://www.huffingtonpost.com/ujwal-arkalgud/why-the-research-industry_b_8256870.html.

[38] Salvo J. Creative disruption and connections drive innovation. 2016. 22 Feb http://experimentsinopera.com/research-and-disruption/.