Designing Interactive Secure Systems: CHI 2013 Special Interest Group

Shamal Faily [a]
University of Oxford
Oxford, OX1 3QD, UK
shamal.faily@cs.ox.ac.uk

Lizzie Coles-Kemp
Royal Holloway
Egham, TW20 0EX, UK
lizzie.coles-kemp@rhul.ac.uk

Paul Dunphy
Newcastle University
Newcastle, NE1 7RU, UK
p.m.dunphy@newcastle.ac.uk

Mike Just
Glasgow Caledonian University
Glasgow, G4 0BA, UK
mike.just@gcu.ac.uk

Yoko Akama
RMIT University
Melbourne VIC 3001,Australia
yoko.akama@rmit.edu.edu

Alexander De Luca
University of Munich
80333 München, Germany
alexander.de.luca@ifi.lmu.de

[a]Primary contact

CHI 2013 Extended Abstracts, April 27–May 2, 2013, Paris, France.
ACM 978-1-4503-1952-2/13/04.

Abstract
Despite a growing interest in the design and engineering of interactive secure systems, there is also a noticeable amount of fragmentation. This has led to a lack of awareness about what research is currently being carried out, and misunderstandings about how different fields can contribute to the design of usable and secure systems. By drawing interested members of the CHI community from design, user experience, engineering, and HCI Security, this SIG will take the first steps towards creating a research agenda for interactive secure system design. In the SIG, we will summarise recent initiatives to develop a research programme in interactive secure system design, network members of the CHI community with an interest in this research area, and initiate a roadmap towards addressing identified research challenges and building an interactive secure system design community.

Author Keywords
Design, Usable Security, Methods, Tools

ACM Classification Keywords
H.5.2 [**User Interfaces**]: User-centered design

General Terms
Human Factors, Security, Design, Engineering

Motivation

In recent years, the field of usable security has attracted researchers from HCI and Information Security, leading to a better understanding of the interplay between human factors and security mechanisms. Yet, designing systems which are both secure in, and appropriate for, their contexts of use continues to be no less a source of frustration. This frustration has now grown to the extent that usability researchers now openly question how security and usability considerations can be incorporated into design practices, e.g. [8, 5]. One of the traditional barriers to carrying out design research in this area has been a glut of practical work evaluating the shape that security and usability design might take. However, as security is now a prevalent concern across all levels of society, we are beginning to see security design research being carried out at many levels, from the board-room [7] all the way down to local grassroots communities [6].

The human-computer interaction (HCI) community is advanced in developing methods to actively engage with users in the design process e.g. participatory design. However, to date, the security community appears to have been influenced very little by such design philosophies, as academic research reflecting upon user-centred design processes for security mechanisms and secure systems is still sparse. Research that does exist is disseminated in a variety of security, software engineering, and HCI workshops and conferences. As a consequence, there is a misunderstanding of the role that different fields play in the design of secure systems. For example, a number of security researchers and practitioners continue to espouse the need to treat *people as the weakest link*, and encourage designers to build systems that *Homer Simpson* can use [4]. Unfortunately, treating users as a problem can limit the opportunities for innovation when people are engaged as part of a solution. Similarly, while extreme characters can be useful for envisaging different modes of interaction, when taken out of context they risk disenfranchising the very people the design is meant to support.

Recent events in North America [1] and Europe [2] have attempted to connect researchers and practitioners across the design, user experience, engineering, and HCI Security communities. These have led to the identification of several different research goals and areas for further work. As a next step, we believe it is important to bring a critical mass of researchers and practitioners together in one place, and explore how these and other as yet unidentified research areas can begin to be addressed. One of the few venues where researchers from these communities come together under one roof is CHI.

Goals of the SIG

The purpose of this SIG is to refocus the usable security community towards the techniques, processes and tools of *design*; these may be concerned with the design of secure software systems, the design of particular security mechanisms and architecture, or design practices in broader socio-technical system. To achieve this, our SIG has three goals. First, we want to present the latest efforts to develop a research programme for interactive secure system design. This is to ensure there is as little ambiguity as possible about the current research "state of the nation". Second, we want to connect those people in the larger CHI community with an interest in interactive secure system design. Finally, we want to develop an initial Designing Interactive Secure Systems (DISECS) research agenda with tangible next steps for addressing identified areas of development while, simultaneously, growing the DISECS community.

SIG Audience

This SIG will target CHI attendees from the user experience, design, and engineering communities with an interest in interactive secure systems. This SIG will allow established researchers to quickly identify who is doing research in what particular aspects of interactive secure system design. This SIG will be of particular benefit to graduate students and early career researchers interested in joining and helping establish a new community within HCI Security around this area. Based on anecdotal comments from prospective attendees, we believe the SIG will also be useful for practitioners who can provide an informed opinion about current challenges they face and research topics they believe need to be addressed.

Agenda

Before the SIG

We will garner interest from possible SIG attendees in three ways. First, we have created a website for the SIG detailing our goals and the SIG's agenda [3]. Second, we will use our own network of contacts, newsgroups, and social media to attract participants to this session at CHI. Finally, in addition to members of the CHI community interested in security, technology design and engineering, we will also reach out to those who seek to understand the role of technology in society. We will also engage those members of the security community with an interest in usability and human factors that might not otherwise consider attending a conference such as CHI. By framing the language of our call to these communities, we hope to encourage traditional non-participants who might otherwise ignore a general call.

SIG Agenda

To meet our goals, the SIG will maximise audience participation and networking through a mixture of plenary presentations, networking activities, and a group affinity diagramming exercise. The 80 minute SIG session will be broken down into the following activities:

- Introduction to the SIG and a synopsis of recent activities to formulate a DISECS research agenda. As part of this summary, we present severeal areas for development identified by these initiatives. These include agreeing key needs and assumptions between communities, engaging designers in thinking about the adversarial element, and stimulating innovation in design techniques and tools (10 minutes).
- Random speed dating session between participants. Each SIG attendee will write 3 points on a postcard: (i) what their DISECS research interests are, (ii) what relevant projects they are working on, or would like to see carried out, and (iii) what research paper or area they find most influential going forward. Participants can either bring these postcards with them, or they can write them up on the spot; postcards will be provided by the organisers. Each participant will also be given a post-it note deck and, for each of their *dates*, participants will complete post-it notes characterising these points on one of the meeting room walls (20 minutes).
- Participatory design activities. Participants will form groups and undertake a number of participatory design activities in order to evolve a better understanding of the identified goals and challenges. The number of activities will vary based on the number of participants, but we hope everyone will participate in multiple activities and spend at least 15 minutes on each (50 minutes).

SIG Outcomes

The outcome of the session will be documented on the SIG website. In addition to any actions decided within the SIG itself, we also envisage two minimum outcomes:

First, the creation of a new online SIGCHI community for Designing Interactive Secure Systems to formalise new and existing networks of researchers. The community's objectives will be agreed in the SIG, and its co-founders will be drawn from SIG attendees who are members of the ACM and SIGCHI. Once it has been setup, the SIG website will become the website for this new community.

Second, the newly created DISECS SIGCHI community will take responsibility for analysing the design outputs from the SIG. We will synthesise insights arising from both this and other notes and observations from the workshop to form the basis of a DISECS research roadmap. The community will solicit volunteers to explore elements of this roadmap in more detail using the most appropriate format; this may be a discussion on the existing HCISec mailing list, workshops at related security or usability conferences, or even a future CHI SIG.

Acknowledgements

The activities described in this paper are supported by the EU FP7 *webinos* project (FP7-ICT-2009-05 Objective 1.2), and the EPSRC funded *VOME* project (EP/G00255X/1).

References

[1] 1st Software and Usable Security Aligned for Good Engineering Workshop. http://www.thei3p.org/events/sausage2011.html, April 2011.

[2] Designing Interactive Secure Systems: Workshop at British HCI 2012. http://diss2012.org, September 2012.

[3] Designing Interactive Secure Systems: SIG at CHI 2013 website. http://disecs.org, January 2013.

[4] Anderson, R., and Fuloria, S. Security economics and critical national infrastructure. In *Economics of Information Security and Privacy*, T. Moore, D. J. Pym, and C. Ioannidis, Eds. Springer, 2010, 55–66.

[5] Bødker, S., Mathiasen, N., and Petersen, M. G. Modeling is not the answer!: designing for usable security. *interactions 19*, 5 (Sept. 2012), 54–57.

[6] Faily, S. Security goes to ground: on the applicability of security entrepreneurship to grassroot activism. *CHI Workshop on HCI, Politics and the City* (2011).

[7] Parkin, S., van Moorsel, A., Inglesant, P., and Sasse, M. A. A stealth approach to usable security: helping it security managers to identify workable security solutions. In *Proceedings of the 2010 workshop on New security paradigms*, ACM (2010), 33–50.

[8] Sasse, M. A. Designing for Homer Simpson - D'Oh! *Interfaces: The Quarterly Magazine of the BCS Interaction Group*, 86 (Spring 2011), 5–7.