Human-Centered Design for Secure Communication: Opportunities to Close the Participation Gap

Ame Elliott
Simply Secure
ame@simplysecure.org

Sara Sinclair Brody
Simply Secure
scout@simplysecure.org

1 Introduction

This talk describes ongoing work in improving the end-user experience of secure communication tools with a focus on identifying barriers to including diverse stakeholders in the usable-security ecosystem. As a first step, we are following a Human-Centered Design research process to conduct semi-structured interviews with a diverse group of stakeholders, including cryptographers, user experience designers, open-source software developers, engineers in corporate environments, and end users [3]. Our presentation shares emerging themes and identifies gaps limiting participation in the design of secure communication tools, including *1*) incentives for motivating adoption by lay users without explicit privacy concerns and *2*) the lack of shared vocabulary for design activities.

2 Background

Simply Secure is a new nonprofit grounded in a belief that technology should respect users desire for privacy and security. Users should not have to choose between services they like and those that are secure, and through collaborations with open-source software projects, Simply Secure works to bridge that gap.

Its a common perception, reflected in the popular press, that existing secure communication tools are unusable, such as TechCrunch's assertion that *nobody has ever figured out how to make [encryption] easy for mainstream users* [4]. The academic and technical communities have a robust track record of research on this topic, from Why Johnny Cant Encrypt through the Symposium on Usable Privacy and Security, the USEC workshop, this event, and others [6].

Our aim is to expand the conversation to include designers and others who have not traditionally participated in scholarly research in a community of practice.

3 This Work

One of the principles of Human-Centered Design is engaging with users from the beginning [3]. As a service organization, Simply Secures users are a diverse group, including open source software developers, engineers, users and their representatives, academic security researchers, user experience researchers, and designers. From Spring 2015, we are conducting semi-structured interviews. Interviews are conducted in a range of settings: in person, remotely, individually, and in groups, while using an iterative approach to adapting the interview guide to probe more deeply on emerging areas of interest [5].

4 Opportunities

This talk shares emerging themes from our current work in progress, specifically exploring ways of engaging designers and end-users in open-source security projects, with the aim of making tools accessible to mainstream users. The talk presents the most relevant gaps for motivating deeper inquiry and opportunities to address the gaps as part of a usable-security ecosystem. Based on work so far, the preliminary gaps are *1*) incentives for motivating adoption by lay users without explicit privacy concerns and *2*) the lack of shared vocabulary for design activities.

4.1 Lay-user adoption

Because communication is inherently social, users are motivated to select tools that allow them to communicate with the people in their networks. Network effects are a powerful opportunity to scale the impact of secure tools, but without consistent use by all parties, secure communication is impossible. Rather than focus on the most at-risk users, such as activists and people in vulnerable geographies, we are researching the needs of mainstream lay users who dont self-identify as having specific security concerns. There is a notable gap in meeting the needs of lay users in a North American context because the level of awareness of security issues is generally low, with popular discourse casting suspicion on any who would use encryption tools [2].

The most compelling reasons to believe in end-to-end encrypted communication tools require understanding of complex issues of network infrastructure that may not be of interest to all audiences. Even recruiting participants for a user study of security tools anchors participants expectations and may artificially foreground security concerns in ways different from natural settings. Best practices in user research can take some steps to mitigate concerns of bias during interviews, but challenges remain [5].

4.2 Shared vocabulary

A challenge to including user-experience designers in discussions about security is the lack of a shared vocabulary for common design activities. Even the phrase usability may mean different things to a user-experience designer than to a usability professional, with designers understanding usability as a specific set of quantitative analyses, rather than as a broader activity. The field of user-experience design borrows language from Human-Computer Interaction, but professionals working in industrial contexts may also use vocabulary from marketing, business, and related domains.

Resources such as *The User Experience Team of One* provide options for standardizing vocabulary and avoiding miscommunications [1]. Clear communication can catalyze designer participation, by helping them scope their contributions to deliver expertise on the most critical barriers to adoption.

5 Conclusions

This talk shares the results of stakeholder interviews to identify gaps in improving the end-user experience of secure communication tools. Initial opportunities include *1*) incentives for motivating adoption by lay users without explicit privacy concerns and *2*) the lack of shared vocabulary for design activities.. Addressing these gaps can increase participation of designers and end-users in the design of secure communication tools so that users dont need to choose between tools they like and tools that are secure. When lay audiences adopt secure communication tools, they contribute to a positive, accessible, people-centered Internet.

References

[1] Buley, L. 2013. *The User Experience Team of One: A Research and Design Survival Guide* Rosenfeld Media, Brooklyn, NY.

[2] Finley, K. 2014. *Online Security Is a Total Pain, But That May Soon Change* http://www.wired.com/2014/06/usable-security/

[3] IDEO.org 2014. *Design Kit: The Field Guide to Human-Centered Design*, http://www.designkit.org/

[4] Lardinois, F. 2014. *Googles End-to-End Email Encryption Tool Gets Closer to Launch*, http://techcrunch.com/2014/12/17/googles-end-to-end-email-encryption-tool-gets-closer-to-launch/

[5] Portigal, S. 2013. *Interviewing Users: How to Uncover Complex Insights.* Rosenfeld Media, Brooklyn, NY.

[6] Whitten, A. and Tygar, J.D. 1999. *Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0.* Proceedings of the 8th USENIX Security Symposium.