Security and usability: searching for the philosopher's stone.

FLÉCHAIS, I. and FAILY, S.

2010

Security and Usability: Searching for the philosopher's stone

Ivan Fléchais
Oxford University Computing Laboratory
Parks Road, OX1 3QD, UK
ivan.flechais@comlab.ox.ac.uk

Shamal Faily
Oxford University Computing Laboratory
Parks Road, OX1 3QD, UK
shamal.faiiy@comlab.ox.ac.uk

> **(...) might there exist a remarkable analogy between this *usable and secure* system and the ancient alchemists' philosopher's stone?**
>
> — Auguste Kerckhoffs *La Cryptographie Militaire* 1883

ABSTRACT

This paper describes the unique challenges facing usable security research and design, and introduces three proposals for addressing these. For all intents and purposes security design is currently a craft, where quality is dependent on individuals and their ability, rather than principles and engineering. However, the wide variety of different skills necessary to design secure and usable systems is unlikely to be mastered by many individuals, requiring an unlikely combination of insight and education. Psychology, economics and cryptography have very little in common, and yet all have a role to play in the field of usable security. To address these concerns, three proposals are presented here: to adopt a principled design framework for usable security and privacy, to support a research environment where skills and knowledge can be pooled and shared, and to guide and inform the principles that underpin the educational curriculum of future security engineers and researchers.

1. INTRODUCTION

The quest for secure and usable systems is neither new nor complete. Even in 1883, Auguste Kerckhoffs was lamenting the failures of the french army to employ a usable and secure cryptographic system [12]. While this treatise is known for expressing one of the most famous cryptographic principles – that a cryptographic algorithm should not depend on secrecy for its strength – the sixth principle also states: *Finally, it is necessary, given the circumstances that command its application, that the (crypto)system be simple to use, requiring neither mental strain, nor the knowledge of a long series of rules to observe.*

The world has now moved on. Issues of security and usability are no longer the province of military cryptographers but of software developers, system administrators, and the user community. Nevertheless, progress in usable security research and design has been slow, due in part to the need to master a large amount of (usually) mutually exclusive, yet necessary, skills and knowledge. To quote from Ross Anderson, "the security engineer needs to understand basic economics as well as the basics of crypto, protocols, access controls, and psychology" [1]. Addressing this fundamental dilemma is necessary if the field of usable privacy and security is to deliver on its promises.

The following sections describe three proposals for the field of usable security and privacy, aimed at fostering a sound design, research and educational foundation.

2. ADOPT A *DESIGN* APPROACH

Relying on individuals to master the many different fields of knowledge necessary for usable security and privacy research is not an option when practitioners need to build systems. Design frameworks are the only means whereby different skills can be utilised and harmonised for the common purpose of building a usable secure system.

EuroSOUPS could solicit and provide a venue for research in usable security design, and encourage existing work to formulate and discuss human-centered security engineering principles and practices.

3. *SUPPORT* AN INTERDISCIPLINARY RESEARCH ENVIRONMENT

Usable security and privacy is a multidisciplinary problem, and supporting a research environment where these disciplines can come together and inform one another is not only desirable but necessary. Like SOUPS, EuroSOUPS can contribute to this research environment by both providing a venue for disseminating research findings and forging new connections between researchers and industry that last beyond an annual event.

We believe EuroSOUPS can play a significant role in the creation of a *network of excellence* for researchers and companies interested in the field of secure usability and privacy. The purpose behind this network would be to facilitate the sharing of knowledge, to identify areas of expertise and to encourage collaboration in the pursuit of new research. Some practical ideas for establishing this network could include:

- the creation of a social network of interested parties,
- a centrally accessible and persistent resource for research knowledge (including experimental designs, research methodologies, questionnaires, lists of individu-

als/institutions with specific expertise in relevant techniques or tools, sources of research funding, the means for groups looking to collaborate on new research projects to identify and approach other partners, etc.),

- an annual meeting at a EuroSOUPS conference to keep the momentum going and provide an approachable venue for people who might be interested in joining.

4. ENGAGE WITH SECURITY *EDUCATION*

There are two aspects to engaging with security education: the first consists of providing useful educational material, perhaps in the form of podcasts or tutorials; the second aims at informing, engaging and shaping different security educational curricula.

- The creation of useful educational material is important to further the cause of usable privacy and security. Disseminating usable security and privacy know-how is predicated on this. Running tutorials or seminars at EuroSOUPS is one means of doing so; another proposal would be to run a *DesignFest* for usable security and privacy—an activity whereby attendees would sharpen their design skills by working on real usable security problems with other participants with different backgrounds and expertise. This type of approach has proven effective and engaging at other venues such as OOPSLA, and provides attendees with a different kind of learning experience.

- Engaging with existing educational curricula requires a clear understanding of the necessary knowledge, skills and techniques that underpin usable security and privacy. Further research is needed to ascertain what these are, and how to best integrate these into the wider security arena, and EuroSOUPS would be an ideal venue for this.

5. CONCLUSIONS

EuroSOUPS presents a new opportunity to shape the field of research in usable security and privacy in order to address current weaknesses. By channelling efforts towards supporting engineering approaches, multidisciplinary research and security education, EuroSOUPS could become a significant European and International forum for furthering the science of usable privacy and security.

6. RESEARCH BACKGROUND

Ivan Fléchais has been researching the problem of how to develop secure and usable systems since 2001. His PhD thesis, supervised by Prof. Angela Sasse and entitled "Designing Secure and Usable Systems" [6], describes *AEGIS*: the first engineering process aimed at supporting developers in creating usable secure systems [7]. Since then, his research has focussed on exploring how to further bring usability and security into the software engineering process, work that has most recently been in collaboration with Shamal Faily. In conjunction with another of his doctoral students, Ronald Kainda, his research into secure mobile device pairing has investigated the security and usability of different pairing methods, and proposed novel ones [8, 10, 9, 11].

Shamal Faily is a doctoral student at the Oxford University Computing Laboratory. Shamal's research involves understanding how existing techniques and tools can be integrated to support the design of usable and secure system. This research has resulted in *IRIS*: a design framework for specifying usable and secure systems [2], the *CAIRIS* tool for supporting this framework [5], and the adaptation of *Personas* to secure systems design [3, 4]. Prior to starting his doctoral research, Shamal spent nearly 10 years as a software engineer at Logica.

7. REFERENCES

[1] R. Anderson. *Security engineering: a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2nd ed edition, 2008.

[2] S. Faily and I. Fléchais. A Meta-Model for Usable Secure Requirements Engineering. In *Software Engineering for Secure Systems, 2010. SESS '10. ICSE Workshop on*, pages 126–135. IEEE Computer Society Press, May 2010.

[3] S. Faily and I. Fléchais. Barry is not the weakest link: Eliciting Secure System Requirements with Personas. In *BCS HCI '10: Proceedings of the 2010 British Computer Society Conference on Human-Computer Interaction*, 2010.

[4] S. Faily and I. Fléchais. The secret lives of assumptions: Developing and refining assumption personas for secure system design. In *HCSE'2010: Proceedings of the 3rd Conference on Human-Centered Software Engineering*, pages 111–118. Springer, 2010.

[5] S. Faily and I. Fléchais. Towards tool-support for Usable Secure Requirements Engineering with CAIRIS. *International Journal of Secure Software Engineering*, 1(3):57–71, 2010.

[6] I. Fléchais. *Designing Secure and Usable Systems*. PhD thesis, University College London, 2005.

[7] I. Fléchais, M. A. Sasse, and S. M. V. Hailes. Bringing security home: a process for developing secure and usable systems. In *NSPW '03: Proceedings of the 2003 workshop on New security paradigms*, pages 49–57, New York, NY, USA, 2003. ACM.

[8] R. Kainda, I. Fléchais, and A. Roscoe. Usability and security of out-of-band channels in secure device pairing protocols. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, July 2009.

[9] R. Kainda, I. Fléchais, and A. Roscoe. *Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions*, chapter Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions. 2010.

[10] R. Kainda, I. Fléchais, and A. Roscoe. Security and usability: Analysis and evaluation. In *Availability, Reliability and Security, 2010. ARES 10. Fifth International Conference on*, 2010.

[11] R. Kainda, I. Fléchais, and A. W. Roscoe. Two heads are better than one: Security and usability of device associations in group scenarios. In *Proceedings of the 2010 Symposium on Usable Privacy and Security (SOUPS 2010)*, 2010.

[12] A. Kerckhoffs. La cryptographie militaire. *Journal des Sciences Militaires*, pages 5–38, 1883.