Seeking the philosopher's stone.

FLÉCHAIS, I. and FAILY, S.

2011

Seeking the philosopher's stone

Article · April 2011

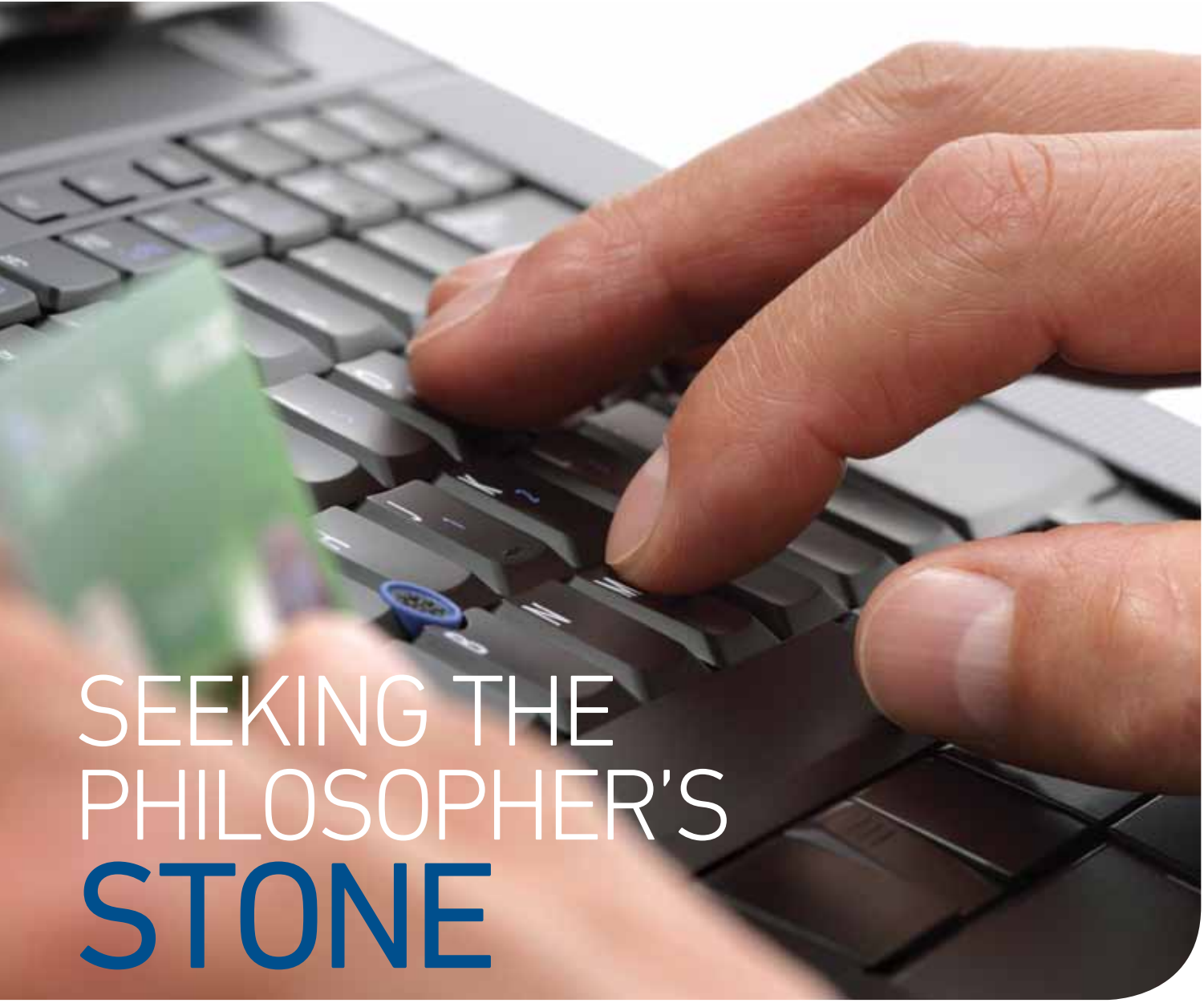
CITATIONS
0

READS
302

2 authors, including:

Shamal Faily
Robert Gordon University
146 PUBLICATIONS **769** CITATIONS

SEE PROFILE



SEEKING THE PHILOSOPHER'S STONE

Ivan Fléchais and **Shamal Faily** of Oxford University Computing Laboratory go in search of the elusive alchemy of systems that are both usable and secure.

Moving usable privacy and security forward

> … 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

This article 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 on 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.

Since 1883 the need for usable security has been recognised

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 (Kerckhoffs, 1883). 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, skill 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' (Anderson, 2008). Addressing

The quest for secure and usable systems is neither new nor complete.

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.

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.

A forum is required to 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.

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 (discussed in the article by Lorrie Cranor), a European network could 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. 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 individuals and institutions with specific expertise in relevant techniques or tools, sources of research funding and the means for groups looking to collaborate on new research projects to identify and approach other partners),
- an annual meeting at a conference, perhaps its own conference to keep the momentum going and provide an approachable venue for people who might be interested in joining.

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 conferences 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 a European network would be an ideal venue for this.

Conclusions

Researchers in the field of usable privacy and security currently have the opportunity to re-shape their field of research in order to address current weaknesses. By channelling efforts towards supporting engineering approaches, multidisciplinary research and security education, a European network could provide a significant European and international focus for furthering the science of usable privacy and security.

ivan.flechais@comlab.ox.ac.uk
shamal.faiiy@comlab.ox.ac.uk

REFERENCES

Anderson, R. (2008). *Security engineering: a guide to building dependable distributed systems*. 2nd edition. Indianapolis, IN: Wiley

Faily, S. and Fléchais, I. (2010). A Meta-Model for Usable Secure Requirements Engineering. In *Software Engineering for Secure Systems*, 2010, SESS '10, 126–135. IEEE Computer Society Press.

Faily, S. and Fléchais, I. (2010a). Barry is not the weakest link: Eliciting Secure System Requirements with Personas. In *BCS HCI2010: Proceedings of the 2010 British Computer Society Conference on Human–Computer Interaction*.

Faily, S. and Fléchais, I. (2010b). The secret lives of assumptions: Developing and refining assumption personas for secure system design. In *HCSE2010: Proceedings of the 3rd Conference on Human-Centered Software Engineering*, 111–118. Springer.

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

Fléchais, I. (2005). *Designing Secure and Usable Systems*. PhD thesis, University College London.

Fléchais, I., Sasse, M.A. and Hailes, S.M.V. (2003). Bringing security home: a process for Developing secure and usable systems. In *NSPW '03: Proceedings of the 2003 workshop on New security paradigms*, 49–57. New York: ACM.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2009). 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*.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010a). 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*.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010b). Security and usability: Analysis and evaluation. In *Availability, Reliability and Security*. ARES 10.

Kainda, R., Fléchais, I. and Roscoe, A.W. (2010c). 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).

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des Sciences Militaires*, 5–38.