R209 Essay: Usable security

Chongyang Shi (*cs940*)

October 17, 2017

This essay provides a synthesis of three papers focused on usable security. While being a subfield of human-computer interaction (HCI), usable security may present a very different set of challenges from broader user-centred design principles [1, Abs.]. Two user-facing security systems were detailedly studied: the user interface (UI) for PGP 5.0 [1] and the airline check-in kiosk [2], in addition to a generalised study on the state of usable security [3].

1 Summaries of research

In order to determine whether security softwares with conventionally well-designed user interfaces can adequately assist novice users in performing complex security tasks, Whitten and Tygar [1] performed a case study on PGP 5.0. After producing a set of definitions and problematic properties of usable security, they evaluated the usability of the UI through two methods: a cognitive walkthrough of confusions facing a novice user of the UI, and user tests conducted with potential users unfamiliar with the software and the PGP concept. The results of their evaluations show that PGP 5.0's UI fails to demonstrate the concepts of email encryption and authentication well, and various problems in visual design can lead to confusions that could result in users performing dangerously insecure operations. However, those critical of this study may consider the choice of PGP 5.0 to be sub-optimal for evaluations, as the protocol design of PGP is significantly more complex than other security tools a novice user may come across, such as symmetric file encryption with a pre-shared key [4]. This may have reduced user performance in user tests.

Herley [3] reviewed the state of usable security research under the contemporary internet context, and found that past efforts in making security components of softwares more usable may have been misdirected. The author argued that many past efforts have overestimated the capacity a user has for completing security-related tasks, and could not produce a usable solution accomplishable with the limited time and attention the user could provide. Exaggeration of average-case security risk [3, 2.3] and creating unrealistic burden of security mandates [3, 1.3] can also lead to the user cutting corners on security. Therefore, the author believes that future research on usable security should be efficiency-focused. While this paper effectively summarised the perceived shortcomings in usable security research, it is relatively thin on detailed recommendations to overcome these problems.

Most recently, Glass et al. [2] studied how the orderings and the transitions between components of a security-related task could impact the usability of the task. Based on the real world scenario of using an airline check-in kiosk, transitions between a set of partially-ordered tasks were modelled as a constraint satisfaction problem (CSP), whose optimal solution in ordering tasks correlated with the best user performance in user tests and the favoured solution by experts surveyed [2, Fig. 7]. This verified the viability of cognitive framework established by the authors. Some limitations of the models were recognised by the authors, the most critical of which is the potential lack of consistency with user expectations on how certain tasks are ordered.

2 Key themes of research

2.1 Sell security to users on incentives, not on endless mandates

A theme observed across the three papers is the need to provide users with good reasons to use security, rather than mandating the users with endless security policies that may result in workarounds and corner-cuttings being invented. Limitations and ineffectiveness of security automations and user trainings were observed by Whitten and Tygar [1, Sec. 1]. Herley noted that security mandates may not convince the users that cost of security compliance is outweighed by its benefits, and that some mandates such as periodic password changes accomplish very little [3, 1.3, 2.2]. Glass et al. also found that when the security mandate (in this case, passport authentication) is placed in the least obstructive way within procedures, users are most satisfied with the process [2, Sec. VII].

2.2 Provide the user with minimal information required for security

It was observed by all three papers that when presented with an overwhelming amount of security information, the user tends to perform less well in accomplish the task. During PGP 5.0 user tests by Whitten and Tygar, too much information about PGP keys, automatically generated trustworthiness levels, or even excessive vocabulary could confuse a novice user [1, 4.6, 4.7]. Herley [3, 2.1] believes that security advices have provided users with too much information to follow effectively. The framework of Glass et al. [2, III. D.] also focuses on improving performance by minimising overall task demand.

2.3 Simplify organisational goals to ease mandates on users

A final theme covered to various degrees by the three papers is the need for policymakers and software engineers to simplify their security goals to reduce the amount of mandates on users. While under ideal circumstances users will sign PGP keys of those they trust, Whitten and Tygar [1, 4.4] believe that this is beyond the abilities of novice users, and hence trust levels should not be prominently displayed by PGP 5.0 by default to avoid confusing these users. Herley [3, 2.4] illustrated the example of avoiding requiring users to choose passwords resilient against offline attacks by adequately protecting hashed passwords stored. By simplifying the organisational security goals without compromising a reasonable level of security, user experience with security procedures can be vastly improved.

3 Ideas of current context

4 Literature review

References

[1] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0." in *USENIX Security Symposium*, vol. 348, 1999.

[2] B. Glass *et al.*, "The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions," *arXiv preprint arXiv:1607.03417*, 2016.

[3] C. Herley, "More is not the answer," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 14–19, 2014.

[4] S. Gujrati and E. Y. Vasserman, "The usability of truecrypt, or how i learned to stop whining and fix an interface," in *Proceedings of the third ACM conference on Data and application security and privacy*. ACM, 2013, pp. 83–94.