securityandtrust.lu

Interdisciplinary Centre for Security,
Reliability and Trust

Luxembourg, 20 May 2019

Evaluation of the PhD thesis:

Usability: Low Tech, High Security

Nikolas K Blanchard, Sorbonne

Examiner: Peter Y A Ryan, University of Luxembourg

The thesis makes a number of interesting and useful contributions to the important but to date rather neglected area of usable security. The last decades have seen an explosion of R&D on security-critical systems, and vast deployment of such systems, largely driven by the advent of the internet. Great strides have been made in the design and analysis of the technical aspects of such systems, the crypto algorithms, protocols etc., but remarkably little attention has been devoted to ensuring that users are able and motivated to interact with them in a secure fashion. This is all the more surprising given that the majority of major breaches are a result of exploitation of the socio-technical aspects of critical systems, social-engineering, users circumventing the security mechanisms etc. This thesis makes significant inroads on addressing these aspects.

The thesis is well-written and a pleasure to read, if a little verbose at times.

**Interdisciplinary Centre for Security,
Reliability and Trust
University of Luxembourg**
6, Avenue de la Fonte
L-4364 Esch sur Alzette

T. +352 / 46 66 44 5667
F. +352 / 46 66 44 5669
snt@uni.lu
www.securityandtrust.lu

Établissement public
Loi du 12 août 2003
Mémorial A149 du 6 octobre 2003
TVA Intracom LU 19805732
N° R.C.S.L. – Luxembourg J20

In more detail:

Chapter 1 provides an excellent state-of-the-art overview of authentication mechanisms.

Chapter 2 describes some experiments on human's ability to accurately transcribe strings of characters and the factors that influence this.

Chapter 3 discusses mechanisms to tolerate common typos when entering passwords. This of course has to be done with great care: such mechanisms assist the user but can also assist the attacker by facilitating his guessing strategies. The trade-offs here are clearly described and investigated and a novel approach to striking an optimal trade-off is presented and validated.

Chapter 4 discusses existing, non-technical approaches to assisting users in generating and recalling (or recovering) passwords. Technical approaches are of course well-known, password safes etc., but the focus here is on techniques that rely on human capacity to recall and perform mental computations, what Manuel Blum calls the "naked man in the desert" techniques. A novel and intriguing and ingenious approach is proposed, "Cue-Pin-Select" that pushes the boundaries in terms of what humans can handle in their head while ensuring good security properties.

Chapter 5 pushes this line of research further by investigating techniques to help users choose "good" pass-phrases, i.e. memorable yet yielding high entropy passwords when used with the CPS techniques of chapter 4.

Chapter 6 describes an interesting investigation of mental computation capabilities.

Chapter 7 presents a number of challenges in the area of secure voting systems, including crucially questions of trust and understandability. It is essential the voting systems not only provide integrity and vote privacy but further that voters, election officials etc., are confident of these properties. This again is an aspect of voting systems that has been largely ignored, even though it is essential for uptake and legitimacy. The chapter goes on to describe some experiments based around Random Sample Voting.

Chapter 8 presents some fascinating ideas to implement Three-Ballot to provide high-assurance without having to rely on software devices to, for example, confirm the well-formedness of a ballot.

This has always been a major obstacle in the implementation of Three-Ballot: how can we verify that a ballot has been filled in according to the rules (two votes for the chosen candidate and one for the others) without violating ballot privacy. This chapter proposed some intriguing, purely physical ways to achieve this.

Chapter 9 investigates similarly "low-tech" techniques to implement high-assurance boardroom voting. As with chapter 8, the goal is to use simple, understandable, i.e. physical, mechanisms to enforce the properties and so avoid having to rely on software etc.

A final, unnumbered chapter discusses open questions and future directions.

Detailed comments:

The thesis is highly original and inventive and demonstrates a remarkable grasp of experimental techniques.

Overall, the thesis thus makes significant contributions to field both in terms of modelling and new designs and implementations. The thesis is very clearly written and structured, I detected hardly any grammatical errors or typos.

In summary, I found the thesis clear and agreeable to read and the contributions to the field of usable, security-critical to be significant and useful. I therefore judge that the thesis be worthy of being defended, and I look forward to the presentation and discussions.

Yours,

Prof Dr P Y A Ryan / peter.ryan@uni.lu