

Département d'Informatique

Paris, 16/04/2019

Pr. David Naccache

✉ david.naccache@ens.fr ☎ +33 7 86 26 76 30

Report on the PhD thesis entitled “Usability: low tech, high security” by Nikola K. Blanchard.

Dear colleagues,

It was a distinct pleasure to read the PhD thesis of Nikola K. Blanchard.

Despite the touching sentiment to see one my most talented undergraduate alumni succeed and complete his higher education, the results are very nice and the document is extremely well written.

The thesis starts with an introductory chapter about the state of the art in authentication.

Chapter 1 is very well written and, as a matter of fact, can be used right away as a course material in the matter.

The second chapter of the thesis deals with the odds to type a password wrongly. The author shows that error rates can vary by an order of magnitude (from 1.9% to 16.9%) depending on the structure of the concerned code. The author shows that many mistakes can be eliminated by using non-ambiguous characters (i.e. characters that cannot be confused with each other and avoiding mixed-case alphanumeric characters). In a way, this observation is intuitively similar to the practice consisting in avoiding the letter “l” and replacing it by “\ell” (which is unconfutable with the digit 1) in scientific papers. The author also studies the effect of spaces in passwords (these reduce friction to some extent) and the fact that users tend to enter and remember CVC (consonant-vowel-consonant) passwords better. Finally memory tests on codes were conducted exploring the ability of users to remember codes after a number of minutes. The future work questions lists very original questions that are likely to trigger further works in the field.

Chapter 2 is extremely well written, the experimental approach is rigorous and the results are consistent with the expectation of intuition.

The third chapter describes what probably what every user would like to have: a typo-tolerant password system. Here we assume that the password is typed with a typographic error and that the system nonetheless manages to tolerate the error and recognize it. This of course trades security against usability (hence the title of the thesis) but Nikola manages to get the best of both worlds by making a typology of errors and developing algorithms that identify the different types of errors (substitution, transposition, insertion, etc) before tolerating them. This is then merged into a complete password verification framework in a very clear and complete way. Section 3.3 analyzes the impact of this feature on security.

The fourth chapter explores Cue-Pin-Select, a system allowing to model passwords after patterns. The author presents three password selection criteria (agent independence, scalability and adaptability). The system is introduced and its resistance to various attacks is explored. The usability aspects of the system are discussed and variants are explored.

The fifth chapter consists in guiding the user in the choice of his passphrases so that the generated phrases are easier to memorize. Here a word choosing software and interface were developed by the candidate and extensive experiments done. Entropy is modelled and estimated and the advantages and limitations of the method are analyzed. The overall result is a large improvement over prior art.

The sixth chapter evaluates the ability of humans to perform various computations and tasks this allows to know to what extent tasks can be used as building blocks to design password schemes.

Chapters 3, 4, 5 and 6 are very interesting and innovating contributions with an important practical impact. The techniques described in those chapters can reduce friction during authentication (burden in case of mistake and memory burden). The experiments are conducted rigorously and the results are clear.

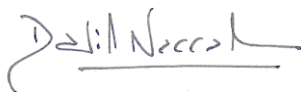
The seventh chapter overviews several modern voting systems and the difficulties in implementing them (section 7.3). The chapter compares different voting systems, their legitimacy and explores the underlying principles of innovative voting schemes (e.g. random sample voting).

Finally, the eighth and the ninth chapters explore “paper & pencil” i.e. non-electronic voting means and propose a number of original constructions.

Chapter 7 is very well written and clarifies the landscape of voting protocols. Chapters 8 and 9 clearly demonstrate creativity and refute the argument that “democracy is expensive”. Using the proposed schemes even poor countries can implement and deploy verifiable voting.

The author has an impressive publication list for a PhD student: 2 journal papers, 6 papers in international peer-reviewed conferences and 5 papers in national peer-reviewed conferences. In addition to those, the author has submitted 8 articles that are currently under review. I would like to underline that this is a very impressive publication record for such a young researcher. In addition many of the works and ideas could have easily been filed as invention patents and have a concrete impact of widely deployed systems.

In conclusion, I recommend **very highly and without any reserve whatsoever**, the defense of this excellent thesis. The works are very original, well researched and well written.



ÉCOLE NORMALE SUPÉRIEURE
DÉPARTEMENT D'INFORMATIQUE
45, rue d'Ulm • 75230 PARIS CEDEX 05

Prof. David Naccache

Membre de l'Institut universitaire de France