DEPARTMENT OF
COMPUTER SCIENCE

Michelle L. Mazurek
University of Maryland
3421 AV Williams
College Park, MD 20742
301-405-6463
mmazurek@umd.edu

Report on the PhD Thesis "Usability: Low Tech, High Security," presented by Nikola K. Blanchard

Dear colleagues,

I am pleased to discuss the PhD thesis of Nikola Blanchard. Overall, the thesis is well written and covers a broad set of interconnected topics, with strong contributions both theoretically and empirically.

Chapter 1 presents a comprehensive survey of authentication, including both the three main categories (what you know, what you have, what you are/do) and overviewing attacker strategies. This chapter effectively and thoroughly covers the space of related literature, providing a useful introduction to a newcomer while also exhibiting depth.

Chapter 2 describes "consonant-vowel-consonant," (CVC) an approach for generating and formatting random codes to make them easier to transcribe (for example when inputting a new WiFi password). The chapter reports on an empirical study with 267 participants comparing CVC to numeric and alphanumeric control conditions. The experiment is nicely designed to investigate the performance of CVC from multiple angles while properly accounting for potential problems such as ordering bias. The results are presented clearly and with helpful graphs that make the large amount of observed data easy to follow and interpret. CVC proved impressively effective, and I think it will have applications even beyond those noted by Mr. Blanchard: for example, as part of authentication ceremonies for secure messaging, or for certain kinds of two-factor authentication.

Chapter 3 presents an error-correction mechanism for allowing servers to accept passwords that contain typos, with a well-specified tradeoff between tolerance and security (accepting more passwords inherently increases the odds of accepting an attacker). The error-correction scheme as designed exhibits nice properties including configurability (so the system administrator can set the risk tolerance) while limiting storage and transmission requirements. The chapter includes a well designed proof (with readable intuition) of the security property of the scheme. It seems plausible to me that a scheme such as this one could see industry uptake, especially for the many well-documented cases where the company in question strongly prioritizes convenience to the customer (see e.g., Florencio+Herley, 2007); this could provide a good design point to help companies achieve the usability they want with less sacrifice of security than is often currently the case.

Chapter 4 presents "Cue-Pin-Select," a human-computable algorithm for choosing unique passwords per account while having to memorize only one passphrase. This chapter carefully reviews earlier work in human-computable passwords before presenting in detail the cue-PIN-select scheme. The chapter also reports on a pilot usability study demonstrating that it is plausible for people to apply the scheme effectively. The provided approach is a nice step forward, as prior attempts that claim to be human-computable have been much too onerous for realistic adoption. The cue-PIN-select technique (and the pilot study) suggest that this scheme may be reasonable for sufficiently motivated users and provides a good starting point for future work continuing to improve usability while maintaining security.

Chapter 5 describes an experiment comparing the memorability of passphrases assigned at random to those chosen from prompt lists of 20 and 100 words. Allow the user to choose from 100 options provided the best memorability, with some sacrifice in randomness (choosing more common or familiar words) but less than might be expected. The experimental results are detailed and clearly presented.

Chapter 6 provides an empirical evaluation (with 81 participants) of a cost model for mental computation previously proposed in the literature but not previously empirically validated. The experiment is well designed and carefully described. The results, although preliminary, cast doubt on the utility of the proposed model; follow-ups to this work could be very valuable both in debunking earlier work that might be used inappropriately, and in setting up follow-on experiments that could be used to obtain a more accurate model for future use. As Mr. Blanchard notes, the availability of a reasonably accurate model would be very useful in allowing some preliminary evaluation of new human-computation schemes, such that many proposed schemes could be understood to be unusable without requiring extensive empirical evaluation; instead effort could be focused only on schemes that are at least plausibly promising.

Chapter 7 provides a useful overview of challenges in voting and elections, focusing on trust, legitimacy, integrity, and secrecy. It also includes two case studies of applying random-sample voting (RSV) among members at conferences. The case studies effectively highlight usability and logistical issues, as well as issues around motivation, that limit the effectiveness of RSV. This chapter lays useful groundwork for further experiments in applying and iteratively improving these voting mechanisms.

Chapters 8 and 9 propose paper-based approaches to realizing secure balloting, for large elections and for "boardroom elections" respectively. In the general election case, the ballot is folded and then marked in some manner. The voter receives a receipt that allows them to check later that their ballot was counted. The poll worker can examine the ballot to ensure that the votes were properly distributed (at most one vote advantage to a candidate) without learning the voter's actual choice. In the boardroom case, voters are able to secretly mark ballots in the same room, and then verify them using a randomly selected pattern that cannot be used for coercion. These chapters usefully catalog building blocks for such balloting approaches, together with constraints that can be used evaluate any such scheme. The chapters lay the groundwork to evaluate the usability of the proposed paper-based approaches in future work.

Overall, the thesis represents an impressive body of work creatively approaching security and usability issues in authentication and voting. It is my pleasure to recommend, without hesitation, that Mr. Blanchard be permitted to defend this thesis.

Sincerely,

Michelle L Mazurek

Michelle L. Mazurek
Assistant Professor, Computer Science and UMIACS
University of Maryland