5 Conclusion and Future Work

We conducted one-on-one interviews and used password analysis tools to gather valuable insights into the complexity of different user passwords. We could trace the evolution of our participants' passwords and the factors that influenced this process.

The results indicate that, in contrast to their first passwords, users today know how to build more secure passwords and thus some current passwords are based on significantly more characters. However, most people still rely on weak (e.g. short) passwords for most authentications, especially, when services are not rated sensitive. In addition, recommender systems and password guidelines had only marginal effects on the password strength and the reuse of old-established passwords is still common.

This is a serious security flaw as attackers could start by finding out a password of a low-sensitivity service, just by guessing or by using some deficiencies of the implementation. The reuse of passwords and the small distances to more secure passwords could consequently enable access to more passwords and more sensitive data. As the growth of web-based services will demand memorizing even more passwords in the future, we argue that usable alternatives to alphanumeric authentication have to be found.

Another point for further investigation is the potential influence of long-term mobile device use on password selection. Text input on such devices is cumbersome, which might, in the long run, negatively influence the security of such passwords.

Acknowledgments. This work was partially funded by a Google Research Award.

References

1. Adams, A., Sasse, M. A., and Lunt, P. Making passwords secure and usable. In Proc. HCI 97, Springer-Verlag (London, UK), 1--19 (1997)
2. Adams, A., and Sasse, M. A. Users are not the enemy. Commun. ACM 42, 40--46 (1999)
3. Riley, S. Password Security: What Users Know and What They Actually Do. Usability News 8, 1 (2006)
4. Shay, R., Komanduri, S., Kelley, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., and Cranor, L. F. Encountering stronger password requirements: user attitudes and behaviors. In Proc. SOUPS '10, ACM (New York, NY, USA), 2:1--2:20 (2010)
5. Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. Of passwords and people: measuring the effect of password-composition policies. In Proc. CHI '11, ACM (New York, NY, USA), 2595--2604 (2011)
6. Proctor, R., Lien, M.-C., Vu, K.-P., Schultz, E., and Salvendy, G. Improving computer security for authentication of users: Influence of proactive password restrictions. Behavior Research Methods 34, 163--169 (2002)
7. Weir, M., Aggarwal, S., Collins, M., and Stern, H. Testing metrics for password creation policies by attacking large sets of revealed passwords. In Proc. CCS '10, ACM (New York, NY, USA), 162--175 (2010)
8. Bonneau, J. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In Proc. SP '12. IEEE Computer Society, Washington, DC, USA, 538--552 (2012)