Literature Review

Aidan Fray

May 23, 2019

1 Research questions

Overall the research will aim to investigate the strength of pEp's Trustword fingerprint mappings, and the ease in which partial collisions can be obtained for keys and how this will ultimately affect the end user(s).

Key areas that will be looked into:

- Is the recommended minimum number of Trustwords enough to provide a basic level of security.
- What attributes make a strong general wordlist for fingerprint mapping and does the Trustword implementation exhibit these features.
- How easy is it to generate similar keys that attack a targeted key pair?
- How can similarity be quantified in terms of words? Does this include pronunciation or visual aspects?
- As usability is the main justification for the use of Trustwords are there alternatives that provide the same usability but with more security?

2 Review

2.1 Fingerprint representation and comparison

Current research in ways to represent and validate fingerprints has almost exclusively focused on the usability of such schemes. The following will individually discuss available research findings alongside a overall comparison of the research recommendations.

The first work in this area was performed by Hsu-Chun Hsiao, *et. al.* in their paper: *A Study of User-Friendly Hash Comparison Schemes*[1] around 2009.

The aim of the study was to provide the first insight into the best encoding scheme used to represent a hash fingerprint. The schemes used were Base32, English words, Random Art[1], Flag[2], T-Flag[3], Flag Ext[4] and finally Chinese, Korean and Japanese symbol encoding.

TODO: Finish review of paper

[1] A scheme proposed by A. Perrig *et al.*[2]
[2] Encoding scheme proposed by C Ellison *et al.*[3]
[3] Yue-Hsun Lin *et al.*[4] improvement on Flag
[4] The author's own improvment on Flag

Work by Dechand Sergej, *et al.*[5] empirically investigated the usability of 4 distinct textual representations evaluated with a experiments involving a total of 1047 participant. The textual representations were: Alphanumeric, Numeric, Words and Sentences. They assessed the number of attacks missed with each scheme alongside results from a questionnaire on the participants preferred scheme and perceived usability.

The paper touches upon issues with decentralised methods of identification such a PGP's Web of Trust and the problems these solutions have with user adoption. These points are made in an attempt to validate the requirement for manual comparison of key based fingerprints. This is a common theme that appears in the majority of the reviewed papers.

Other references made within the paper touch upon the vulnerabilities and usability issues present with the way humans interact with the security systems. Example of these are studies showing humans find it difficult to comprehend long and "meaningless" strings and the lack of actual comparison performed by actual users in live scenario's. These are, however, acknowledged as limitations in the later stages of the paper.

The paper has defined the upper and lower bound costs of the attacker's resources and strength as $610K to $16B, with an ability to control 80-bits of the fingerprint. This in comparison to other papers is high and is almost encroaching into the realm of a highly sophisticated attacker. Therefore, the lack of consideration for the lower-end of the attack resource spectrum can be considered a limitation of this study.

Overall, findings from the paper state that conventional encodings such as Hexadecimal and Base32 perform worse than all other alternatives in a realistic threat model with over 10% of users failing to detect an attack on these encoding schemes. The recommendations of the authors is to to replace these encoding schemes with Words or Sentences due to their very high success rate and high usability scores.

References

[1] H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H. Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A study of user-friendly hash comparison schemes," in *2009 Annual Computer Security Applications Conference*. IEEE, 2009, pp. 105–114.

[2] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security," in *International Workshop on Cryptographic Techniques and E-Commerce*, 1999, pp. 131–138.

[3] C. Ellison and S. Dohrmann, "Public-key support for group collaboration,"

ACM Transactions on Information and System Security (TISSEC), vol. 6, no. 4, pp. 547–565, 2003.

[4] Y.-H. Lin, A. Studer, Y.-H. Chen, H.-C. Hsiao, L.-H. Kuo, J. M. McCune, K.-H. Wang, M. Krohn, A. Perrig, B.-Y. Yang *et al.*, "Spate: small-group pki-less authenticated trust establishment," *IEEE Transactions on Mobile Computing*, vol. 9, no. 12, pp. 1666–1681, 2010.

[5] S. Dechand, D. Schürmann, K. Busse, Y. Acar, S. Fahl, and M. Smith, "An empirical study of textual key-fingerprint representations," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016, pp. 193–208.