Project Plan

Aidan Fray

June 14, 2019

1 Title

"Security evaluation of pEp's TrustWord implementation"

2 Motivation

- Use-case for TrustWords: Users are often deterred by difficulty in key authentication and end-to-end encryption (e.g. PGP web-of-trust).
- Other word lists result in a higher number of words to compare. Trustwords mapping of a word to 2 bytes results in a lower number of words. Meaning the possibility of increased usability
- However, the mapping of words to 16-bits is yet to be proved as secure as this is the **highest number of bits per word**s seen in the literature. This results in the number of words required being higher than that of the users' vocabulary and even the number of total words in the respective language.

3 Goals

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). This will be accompanied by recommendations into how the TrustWord system can be altered to provide increased security alongside research into what makes an effective wordlist.

4 Possible research questions

- 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?
- What are some of the most effective ways of measuring linguistic distance or similarity?
- How easy is it to generate similar keys that attack a targeted key pair?
- How can the search for similar keys be assisted? Could weighting them like "*Fuzzy Fingerprints Attacking Vulnerabilities in the Human Brain*" help to find partial matches?
- 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 does the increase in usability justify the hypothesised reduction in security?

5 High Level View

5.1 Trustword attacks

5.1.1 Similarity metrics

This section will discuss the feasibility of attacking 4 Trustwords. This will require "similar" words to be detected in the dictionary. Therefore, "similarity metrics" will be required.

Due to the defined use-case of Trustwords to be authenticated over a audio based channel, metrics that measure the pronoucability of a word will be used.

[**FURTHER WORK: Using metrics that consider the visual aspect of a word - this could be useful due to in-person authentication**]

- Soundex
- NYSIIS
- Match Rating Approach
- Word Vectors
- Combined (With Levenshtein distance)

[**TODO**] **Experimentation:** Trimming down these metrics might be required with a quick pilot where I attempt to measure the user-perceived similarity accuracy of the schemes. What could be considered is the number of permutations and the "perceived" similarity.

5.1.2 Similar list creation

These metrics then can be used to substitute in place of other words to create a list of near-collision matches/permutations. These will help well generating near-collision keys.

CONSIDERATION: The method works by incrementing the exponent? How does this affect the structure of the key

5.1.3 Tool design and creation

Discussion will occur here around the creation of the tool. Will need to talk about the inspiration of the tool (Scallion) and the improvements made over it:

- Benchmark of comparison of large number of keys.
- Why C++ was used?

5.1.4 Study into the effectiveness of the matches

The could be with the pilot where the results are extrapolated. There are two ways to run this study:

1 Actual matches are computed and compared

2 Evaluation of complexity is computed prior, and for the experiment is simulated.

I think actually showing the matches can be actually computed and simulating them in the study gives the best balance. [Option 2]

Would I also want to do this with a random single target key? Or the worst case scenario. There are keys that have a higher number of potential matches, this is due to the words the key's fingerprint is mapped to.

5.1.5 Conclusion of Trustword security

This will have a conclusion stating the security of the minimum recommendation of 4 Trustwords.

[FURTHER WORK: Evaluation with a higher number of words]

5.2 Improvement study

This is recommendations into improvements with Trustwords. This will pretty much revolve around the word vectors and their ability to allow wordlist "strength" to be quantified.

Word vectors

The strength of the metric was shown in it's own paper with comparison with another famous study into an empirical way to vectorize words. This could even be linked back to the initial pilot study.

[FURTHER WORK: More evaluation into the effectiveness of the word vector method]

Choice of Trustwords

- Homographs (Spelt the same by pronounced differently)
- Homonyms (Different spelling same pronunciation)

Here I could make recommendations through improvements on the word lists:

- Reduce the size of the wordlist (8bit (256 words)/10bits (1024 words))
- Different choice of words
- ?

These could then be evaluated in a similar way to show possible improvements over the base wordlist used by Trustwords

[**FURTHER WORK: Other languages found within Trustwords require this evaluation**]