Paper Notes

Aidan Fray

May 20, 2019

TODO: Need to find papers on study of words are a comparative measure.

OVERVIEW

- Lots of research performed on E2E applications (Telegram, WhatsApp etc)
- Lots of study into overall representations of fingerprints

1 Can Unicorns Help Users Compare Crypto Key Fingerprints

This paper tested 8 different fingerprint representations with 661 different participants. All of these representations are testing using compare-and-confirm (basic comparison process for fingerprints) and compare-and-select (select from a list)

- Hexadecimal
- Alternating vowel/consonant
- Words
- Numbers
- Sentences
- OpenSSH visual host key
- Vash
- Unicorns

The paper also emphasises the attention that has been taken to realism in the experimentation stage.

Talks about long term usability issues with public-key crypto and states fingerprints are a main source of the problem. ([28])

There seems to be mixed findings with compare-and-select and compare-and-confirm ([14, 17])

There has been research into OpenSSH fingerprints and how users interact ([19, 24])

Paper chose to target a security level of 160-bits

Papers attack strengths were 2^{40}, 2^{60} and 2^{80}

Paper states that MTurk users have been shown to be younger and better educated than the general US population ([15])

1.1 Findings

- Graphical representations have mixed success rates (with quick comparison times)
- Recommendations not to use **compare-and-select**
- **No method** really provided enough security for high risk situations, they recommend removing users from the loop by using smart phone cameras etc

2 An Empirical Study of Textual Key-Fingerprint Representations

Study involved 1047 participants evaluating 6 different textual representations on MTurk. The study also includes an evaluation into usability.

The study has an attacker power of around 80 of 112 bits.

- X

More mention to decentralised method finding it hard to find adoption such as Web of Trust and Namecoin ([7, 13, 30])

References as system called CONIKS and others ([24, 39, 27]) that aim to provided a directory of keys

States that many systems still rely on fingerprint comparison ([17])

States that the **hexadecimal** encoding is used in most systems.

States again that fingerprint comparison is seldom done in practice ([17, 37])

Studies have shown that users find it difficult to compare long and "meaningless" strings ([19])

References to other word lists used. PGP Word list [22] and english word list compiled by K.C. Ogden [31]. The Peerio word list is generated from the most common words in english subtitles.

Interesting recommendation into the use of *scrypt* [34] and *Argon 2* [3] can be used to shorten the fingerprint length. These work slowly and a prevent easy computation of pre-images.

When generating partial-collision fixing the bits at the start and end has been shown a best practice ([17, 37])

2.1 Findings

- Overall recommendation is to replace **hexadecimal** with **sentence** based encoding
- Findings show that **hexadecimal** and **Base32** perform worse than the other alternatives in realistic threat models. With over **10%** of users failing to detect attacks with these schemes.