Paper Notes

Aidan Fray

May 22, 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.

- Alphanumerical
- Numerical
- Words
- Sentences

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.
- According to their study, **words** and **sentences** we some of the best methods for avoiding attack
- Words has the second highest usability ratings second to only sentences

3 Usability and Security of Out-Of-Band Channels in Secure Device Pairing Protocols

Paper looks into the positives of secondary channels used to authenticate device pairing. Such as device fingerprint comparison. It also aims to look into the fact that many studies performed do not take into consideration the aspect of human interaction.

Total of 30 paid participants were recruited where the experiment simulated a P2P payment system.

They collected:

- Time to completed the associated process
- Number of security or non-security related errors

And quantified using questionnaires:

- Ease of use with the representation
- Satisfaction with time spent with a method/representation
- Participant's confidence with the scheme

The paper also tested methods:

- Compare and Confirm
- Compare and Select
- Compare and Enter
- Barcode scanning

Representations:

- Numerical
- Alphanumerical
- Words
  - Dictionary of 1024 words each mapped to 10-bits
- Sentences
- Images
- Melodies
- Sound (Numerical/Alphanumerical)

"People are the weakest link in the security chain" [26]

Mentions a normal channel as a "Dolev-Yao" channel [5]. This is where an attacker can overhead, delete and modify messages.

Talks about systems that were secure on paper that ended up in practice being miss-handled to reduce security. One example is with the Russian army in WWI [1]

Bruce Schneier [27] also argues that systems and involves humans therefore often systems are broken due to improper use.

3.1 Findings

- Showed for **usability** methods ranked:
  - Comparing-confirm
  - Typing strings
  - Comparing-select
  - Barcode
- Showed for **combined security** and **usability** methods ranked:
  - Typing strings
  - Barcodes
  - Comparing-confirm
  - Comparing-select

  Showed that the best methods in terms of the SUM score [24] ranked the top 3 as:
  - Numeric(C&C) [73.7]
  - Alphanumerical(C&C) [72.5]
  - Words (C&C) [70.6]

  Numerical had 0% security failures, Word 3.3% and Alphanumerical had a high 13.3%

  NOTE: This is a very small sample size.

4 SafeSlinger: An Easy-to-use and Secure Approach for Human Trust Establishment

The aim of SafeSlinger is to solve the issue of key exchange. They aim to leverage the initial personal contact of people to facilitate trust. To solve the issue of people that would never meet they implement a system of "shared acquaintance"

Talks about issues with decentralised (PGP [42]) and centralised (SSL CA [27, 34]) key exchange.

"Tim Berners-Lee has called upon security researchers and professionals to design a public key encryption system for the people [11]"

Only uses **24-bits** of a SHA-1 hash of all the exchanged information, **could this be exploited?**