Paper Notes

Aidan Fray

May 25, 2019

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

Lots of research has been done into the secure pairing of devices with minimal human involvement:

- Using Camera Phones for Human-Verifiable Authentication
- Loud and Clear: Human-Verifiable Authentication Based on Audio
- A human-verifiable authentication protocol using visible laser light
- Secure Device Pairing based on a Visual Channel
- NFC
- Physical contact

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 On the Pitfalls of End-to-End Encrypted Communications: A Study of Remote Key-Fingerprint Verification

Paper compares the fingerprint verification task in the context of Instant messaging E2E The paper is also choosing to focus on the remote vs proximity ways of comparing fingerprints. They aim to study the security and usability of human-centred E2E key verification. The study ran with 25 participants.

Seems to be the first study of remote code verification study

Study compares Numerical, Image and verbally spoken codes and QR just for proximity alongside all the other alternatives.

The studies main aim to compare remote to proximity, not compare the various methods

The research is split into two sub-goals: Robustness - looks at the FAR and FRR. User experience and perception - System usability, Comfort, Satisfaction and Adaptability

States that numerical is the one of the most common representations, but out of the chosen methods 50% use numerical and the rest hexadecimal?

They included 3 level of incorrect codes. One char change, one block and the entire fingerprint

Overall Audio was one of the most secure and easiest to use. However results for image based comparisons were not controlled in any way due to the author being unable to access the telegram image generation, this means while the other schemes had controlled restraints the image did not. Images was rated the worst.

Findings:

- High False Acceptance Rate (False Negative) for all code verification methods
- Results point to low usability in remote code verification settings, aside from audio based verification ever scheme has above 20% False Rejection Rate (False Positive)
- In proximity settings users were able to detect attacks with minimal error rates

3 The drunken bishop: An analysis of the OpenSSH fingerprint visualization algorithm

The aim of this research is to study the OpenSSH Visual Host Key. The authors claim that the scheme was heuristically designed and has very little backing in terms of formal research, this paper aims to create a foundation for this research.

OpenSSH uses MD5 to generate a 128-bit fingerprint of the Server's key, this is then split into 64 2-bit pairs. These are then traversed byte wise in a right to left over the bit pairs. Each pair defines the direction of travel. If the snake reaches a position multiple times a pre define character is added depending on the number of visits (for example, 6 times == "B")

The paper also discusses ways to create collisions:

In conclusive results and more of an inital PoC

- Brute force
- Graph theory
- Brute forcing a visual set

4 Improving the Robustness of Wireless Device Pairing Using Hyphen-Delimited Numeric Comparison

In the context of secure device pairing the paper aims to improve the human interaction with number pairing.

Lots of research has gone into Short Authentication String (SAS) numbers ([14], [10], [4])

The research was peformed on very old devices. Nokia 6030b, very out of date and not reflective of anything around at this time.

Usability study looked into Efficiency, Robustness, General Usability

Strange format of keeping the numbers exactly the same but just placing hyphens in the middle. The authors attempted to remedy this by spacing the experiments with a days gap

Study was performed with 40 participants

Very small number of values tested only 5 overall???

Initial results show promising results for hypen delimitations etc alongside improved user impressions

5 Loud and Clear: Human-Verifiable Authentication Based on Audio

Paper is in the context of secure device pairing. The paper proposes the use of Loud-and-Clear which uses text to speech to vocalise a robust english like sentence derived from a public key

"Stajano and Anderson proposed a method for establishing keys by means of a link created through physical contact [9]."

"A number of efforts have been made to involve a human user in the secondary channel in order to manually verify/compare keys (or hashes thereof) including [24, 11, 12] and [21]."

CHECK: Manual authentication for wireless devices.

"system represents a cryptographic hash as a series of six short (up to four-letter) words" - N. Haller. Rfc1760: The s/key one-time password system, 1995.

System truncates the hash and encodes into 10-bit sections.

The system is based of MadLib sentences that are used mainly as amusment for children where gaps in text are filled with nouns

The effort placed into making an order for the wordlist is similar to that of PGPfone. They effectively want to make sure that one bit change, results in a completely distinct word

The paper is not backed up by any empirical data and is just a technical description on the system. It included just a performance analysis.

6 Whole-Word Phonetic Distances and the PGPfone Alphabet

PGPfones designed solution was the development of a wordless based of military NATO codes.

The authors used Moby Pronunciator database of nearly 200,000 word/pronunciation pairs.

Use-case for these findings are when verification needs to occur over a auditory line.

Mentions on potential further work in the emprical evaluation of these points

TODO: An analysis of perceptual confusions among some English consonants