Paper Notes

Aidan Fray

May 29, 2019

1 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?**

2 Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal

Papers overall aim is to study and then improve the ease and provide motivation for users to complete the authentication ceremony in Signal IM. The authors apply what they refer to as "Opinionated design" to naturally assist users in completing the authentication ceremony.

"Two recent papers demonstrated that with some instruction about the ceremony itself [8] or the importance of comparing keys [20], users can successfully find and use the authentication ceremony. However, users still took an inordinate amount of time—over 11 minutes on average—to find and complete the ceremony [20]."

That paper showed increases in the number of users actually completing the

ceremony.

Work was inspired by a study by Vazirpour et al *"Is that you, Alice? a usability study of the authentication ceremony of secure messaging"* [COMPARE RESULTS]. They also borrow some methodology from this work.

The paper's actual modification are inspired by work from *"When SIGNAL hits the fan: On the usability and security of state-of-the-art secure mobile messaging"*

3 Use Your Words: Designing One-time Pairing Codes toImprove User Experience

The use of works instead of numerical codes. This is in the context of device pairing in IoT. Something that is new in the literature

Search space required was 500,000,000

Numeric: 9 digits Alphanumeric: 5 chars Words: 3 words

Paper contains references to lots of research into words distributions etc

Paper claimed that 800 works would need to be used but in the experiment only utilised 242 words???

Words provided a faster entry time with no reduction in accuracy

"It is known that typing familiar words is faster than typing random strings [22]"

Paper did not consider malicious aspect of their methods, no discussion was made into how a dictionary of 800 words could be easily impersonated

However, promising results for the usability of word based encodings on displays with low fidelity

4 Whole-Word Phonetic Distances and the PGPfone Alphabet

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

Key terms: "Phonetic confusability"

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.

Words are created from "phonemes" (Unit of sound in a word). They state the the distance between two words can be approximated by between the phonemes that make up the word.

"It should be noted that this is only one of many possible approaches."

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

"A larger list (two bytes per word) would require nearly 650 kilobytes of memory, as well as a word vocabulary larger than most speakers' vocabulary."

Big assumption that the two word PGP word list will be memorised by people "This assumes, of course, that the (listening) human can tell from which list a word has been drawn.". However, I think this was rectified with the 2-syllable then 3-syllable trick for even odd words.

Many questions proposed by the author:

- Do the pronunciation assumptions fail when the reader is not a native English speaker?
- How confusable are the words?