Paper Notes

Aidan Fray

May 27, 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"*