Research Seminar in Cryptography

Benson Muite

benson.muite@ut.ee
http://kodu.ut.ee/~benson

7 September 2016

Password Managers

- You will perform a survey of available password managers. Determine their security (you will need to be able to examine their code to do this) and user friendliness. Example password managers are
  - KeepassX (`https://www.keepassx.org/`)
  - Keepass (`http://keepass.info/`)
  - Pass (`https://www.passwordstore.org/`).
- If you have time, write something better.

Secure Hardware

- Genkin et al. 2016 http://dx.doi.org/10.1145/2851486 give an overview of methods used to extract cryptographic keys from personal computers by making physical measurements during the execution of a mostly known algorithm. Read the article and some of the references. Choose one attack to setup and reproduce. Consider trying the reproduction on devices other than personal computers, such as smart phones.

Secure encrypted email

- Compare and contrast the approaches to secure encrypted email, for example as taken by pgp (pretty good privacy `https://tools.ietf.org/html/rfc4880`) and tutanota (`https://github.com/tutao/tutanota`). You should examine both user friendliness, theoretical underpinnings and an actual implementation.