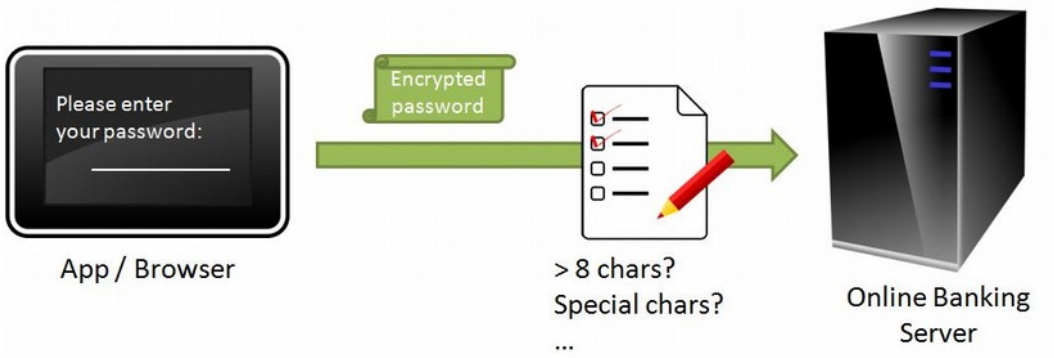
Master-Thesis

TECHNISCHE UNIVERSITÄT DARMSTADT

Secure Online Banking with Homomorphic Encryption

1. General Information

A homomorphic encryption scheme allows for computation on encrypted data. Users or machines can execute computations on encrypted data without getting knowledge about the plaintext data.
In the password (PW) login work flow to an online banking system, policy checks (e.g. length of a PW, type of included characters) must be performed, in order to compare whether the PW fulfils certain security criteria. If end-to-end encryption of passwords is in place, those policy checks can be performed on encrypted data using homomorphic encryption.



2. Goals

Setup of a formal model of the login work flow, including policy checks, is the first step. The second step is the selection and potential adaptation of a suitable homomorphic encryption scheme. In addition, a prototype application shall be implemented.

3. Required Skills

The required skills, in order of importance, are:

- basic knowledge on encryption schemes (especially lattice-based encryption)
- knowledge in linear algebra
- programming skills
- knowledge on homomorphic encryption will be helpful

Knowledge of the English language is required to get along with the technical literature. Theses should be written using LateX.

4. Contact

If you are interested, please contact
Rachid El Bansarkhani
mail: elbansarkhani@cdc.informatik.tu-darmstadt.de
Michael Schneider
mail: mischnei@cdc.informatik.tu-darmstadt.de