
- Master/Diploma thesis - Security of Hash Functions in Electronic Voting

CASED

In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on www.cased.de.

Motivation & Goal

In remote electronic voting systems there is a need to improve usability while maintaining acceptable security levels. In the context of remote voting, voters interact with lengthy and cumbersome hash values in order to verify their vote. Voters are unlikely to opt for the verifiability techniques available as they are difficult to use and if they opt for verifiability the required steps are error prone.

In this research work therefore, we aim to shorten hash values in order to make them more usable, analyse what lengths are considered secure given different election settings, as well as develop automated alternatives for vote verification such as based on QR codes and mobile phones. This third goal should also ideally be appropriate to verify fingerprints of SSL certificates and PGP keys. This work will be based on previous work of the group on the Helios voting system (www.heliosvoting.org).

Requirements

- High motivation and creativity;
- Strong interest in electronic voting research;
- Broad knowledge of cryptographic models and in particular hash algorithms;
- Experience with reading research papers;
- Knowledge of the English language.

Start Date

1st August, 2011

Contact

If interested, send a motivation letter and a CV (including exam results) to:

Maina Olembo, SecUSo

CASED, Mornewegstrasse, Room: 4.2.12

E-Mail: maina.olembo@cased.de

Office hour: Thursdays, 16.00 – 17.00