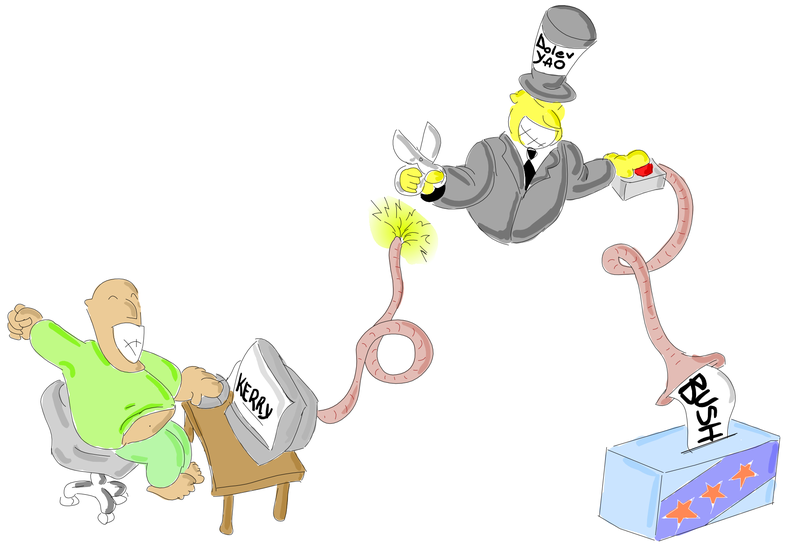
Language Based Technology
Informatics and Mathematical Modelling

Static Validation of Voting Protocols

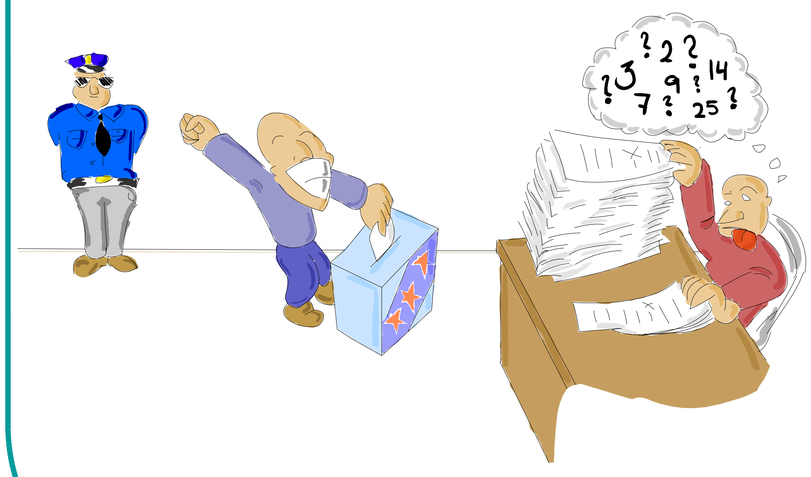
Esben H. Andersen & Christoffer R. Nielsen

Due to the rapid growth in computer networks, most people nowadays have access to the internet. This makes electronic voting a viable alternative to the classic paper vote for governmental elections as well as small scale elections and surveys. However, the use of electronic voting systems introduces new ways to systematically disrupt the vote or falsify the result. If these systems are to replace the classical way of voting, the communities that hold the elections, should be convinced of their correctness.



We have developed a framework for automatically validating the security properties of voting protocols. The framework uses a process calculus in the LySa-family to model the protocols. The analysis uses this model to approximate the behaviour of the protocol in presence of an arbitrary attacker as described by the Dolev-Yao condition.

The framework has been used to successfully validate four of the five security properties for three different voting protocols; namely FOO92, Sensus and E-Vox.



The security properties for electronic voting systems differ from those of ordinary key-distribution protocols and can be formalised into five main properties:

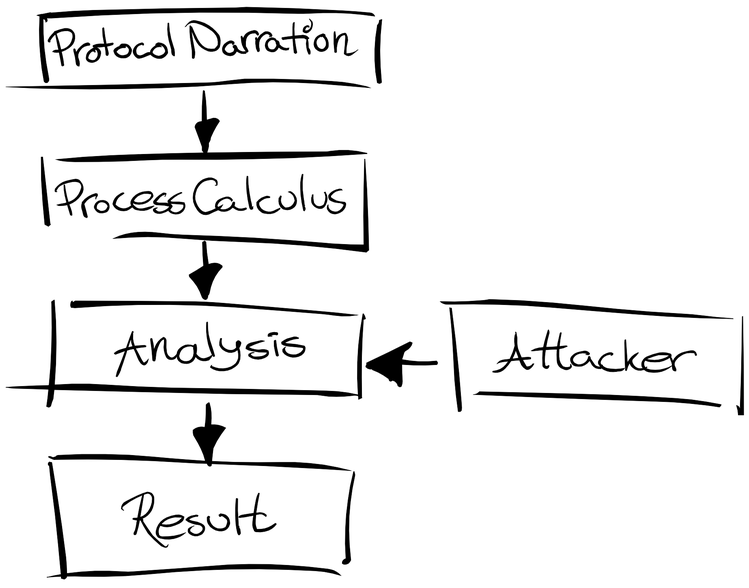
Verifiability: Voters can verify that their votes have been counted.

Accuracy: (1) No votes can be altered, (2) validated votes count in the final tally and (3) invalid votes cannot be counted in the final tally.

Democracy: (1) Only eligible voters can vote and (2) eligible voters can only vote once.

Fairness: No early results from the voting can be obtained.

Privacy: Voters and their votes cannot be linked together.



Supervisor: Hanne Riis Nielson

IMM-M.Sc-2005-55