Protection Against Hackers on Client Computers for e-Voting Systems

Gorm Salomonsen
Cryptomathic S.A.
Gorm.Salomonsen@cryptomathic.com

Recently, Ivan Damgaard and Mads Jurik proposed a protocol for protecting Internet voters against hackers. The protocol ensures that hackers with full control of the computer of a voter will be unable to see what the voter votes. Further, if the hacker tampers with the vote and tricks the voter to vote for a different candidate, the vote will be for an arbitrary candidate (uniformly distributed on all candidates) rather than for the choice of the hacker. This solves a principal problem, which has been a showstopper for some voting projects. However, when this protocol is combined with secrecy of votes implemented using homomorphic encryption and secret sharing, the performance is not good enough to make a practical implementation of the protocol for elections with a non-trivial number of voters and candidates.

In the talk I will present recent work, which is joint work with Jens Groth, where we work on trading performance of the protocol against small, well-defined, security weaknesses. The weaknesses will be of the form that a hacker with some knowledge can get some well-defined probability of guessing what a voter voted or of influencing the election in the way he desires. By setting parameters, these probabilities can be made as small as desired on the cost of additional computational effort.

The constructions are quite general, but will be presented in the context of the generalized Paillier crypto system with a particular system of non-interactive zero-knowledge proofs for implementing a secure voting protocol. This system was proposed by Ivan Damgaard, Mads Jurik and Jesper Buus Nielsen in 2001 and is efficient enough to make elections with secrecy and non-trivial numbers of voters and candidates feasible.