Cryptology ePrint Archive: Report 2011/341

An Improved Internet Voting Protocol

Mehmet Sabir Kiraz , Süleyman Kardaş, Muhammed Ali Bingöl, and Fatih Birinci

Abstract: Norway is going to experience an Internet voting scheme in September 2011 for local governmental elections, targeting a comprehensive Internet voting system in 2017 for national election. This protocol is strong from several aspects. First of all, it resists against malicious voter's computers. Namely, an honest voter will be aware of a malicious behavior caused by the computer during the entire voting procedure. However, the security of the protocol depends on the assumption that the players (organizations) are completely independent and reliable, and the receipt codes are sent to the voters securely. In this work, we take a closer look at the Internet voting protocol and investigate the followings: – The privacy of voters are compromised if there is a cooperation between the players Ballot Box (BB) and Receipt Generator (RG) since the private key of Decryption Service (DS) can be obtained by the two former players. To prevent this possible issue, we propose an improved protocol without adding additional players. – To verify the correctness of the overall protocol two additional channels are used where receipt codes are sent to the voters over the pre-channel (e.g., postal service) and also sent over the post-channel (e.g., SMS). However, if a voter holds both SMS and the paper of receipt codes at the same time, he can reveal his/her vote even after the election. To overcome this issue, we propose a new method where the SMS is used only as a notification message, and an additional phone call is used for the complete verification of the vote. – The reliability of the Norwegian scheme is based on the correctness of the receipt codes that are sent to the voters over a secure prechannel. However, if the printed receipt codes are falsely generated (or falsely printed) or the pre-channel is not completely secure, a vote can be counted for different candidates without any detection. In order to prevent this problem, in our protocol, the voters also take a part in the verification of the receipt codes before the vote casting protocol.

Category / Keywords: cryptographic protocols / Internet voting, Voting privacy, Threshold cryptography, Homomorphic encryption

Date: received 23 Jun 2011

Contact author: m kiraz at uekae tubitak gov tr