Chapter XVII

Anonymous Code Lists for Secure Electronic Voting over Insecure Mobile Channels

Nico Voutsis, Hewlett-Packard, Switzerland
Frank Zimmermann, Hewlett-Packard, Switzerland

Abstract

A protocol is proposed that would allow electronic voting over channels, which typically are regarded as insecure like short message service (SMS) and cellular phones. Unlike personalized lists of codes, which are typically proposed to secure the vote and to uniquely identify the voter, we propose anonymous code lists, which offer more flexibility and security, in particular with respect to privacy and the anonymity of the voter.

Introduction

Back in January 2003, the state of Geneva, Switzerland, performed the first official e-voting over the Internet. In the period before and during the ballot period and also in the subsequent ballots, the solution went through a thorough security analysis and extensive testing (Geneva, 2005). Due to the intense spread of cellular phones...
and other mobile appliances for data communication, an additional requirement arose, to also enable voting over these channels, which typically are regarded as insecure. This requirement motivated us to develop a communication process and algorithm for “secure electronic voting” over “insecure mobile channels” based on “anonymous code lists”.

This chapter discusses the key requirements and proposes a technical solution for enabling the “secure electronic voting”. We regard the electronic voting through any channel as an additional means for voting rather than a replacement for the traditional paper-based solutions, like voting at the poll site or postal voting. Therefore, this chapter does not discuss the political and social context and consequences of introducing electronic voting.

The chapter is organized as follows: in the next section, the key requirements are summarized, and the third section discusses how these requirements are addressed by the proposed solution. The fourth section describes in detail the e-voting protocol based on anonymous code lists. The final section contains our conclusions.

### E-Voting Definitions and Key Requirements

What is e-voting? The so-called e-voting denotes any mechanism used to cast a vote or to participate in elections, by which the relevant data are transmitted over a network (Internet or mobile network). In most cases, e-voting represents an additional voting channel and its use is not mandatory. It underlies the same requirements with respect to security as the conventional voting and election procedures at the poll site or for postal voting (see Warynski, 2003; Zimmermann, 2003).

The most critical security requirements are:

1. Only registered and authorized voters are able to vote.
2. Each voter has one and only one vote. No one can vote more than once, even if various channels are available.
3. Voters are protected against identity theft. No third party is able to vote on behalf of an authorized voter.
4. The votes are secret and not known before the official ballot reading and tallying.
5. Vote secrecy and anonymity is guaranteed. That is, voting is anonymous, and it is not possible to associate a voter with his or her vote.
e-Government Adoptions in Developing Countries: A Sri Lankan Case Study
[www.igi-global.com/article/e-government-adoptions-in-developing-countries/103892?camid=4v1a](www.igi-global.com/article/e-government-adoptions-in-developing-countries/103892?camid=4v1a)