University of Fribourg / Faculty of Science and Medicine / Department of Informatics

Broadcast Channel With Memory and Bulletin Board

From Theory to Practice

Severin Hauser

A good way to ensure trust in applications like e-voting is to make the processes verifiable by everyone and it is nowadays often considered a Must-have for an e-voting application. Cryptographic protocols normally use *proofs* to demonstrate that all involved parties acted according to the protocol. This makes the protocol verifiable but only to the parties that are in possession of the corresponding proofs. To solve this problem the protocols often assume that a so-called *broadcast channel with memory* exists. This is a channel that reaches everyone and can at any time present to anyone a full transcript of all the messages sent over it. Unfortunately there exists no real-world implementation for such a channel and therefore other solutions must be explored.

First a definition for such a broadcast channel with memory based on a model of parties and channels is presented. Because there is no implementation that covers this definition a model of a *bulletin board service*, which is a service that aims to provide the same functionality and similar guarantees, is developed. This service is administered by one or more parties and for the service to work one must trust some of these parties to be honest. To understand which parties to trust for which guarantee in an implementation, the roles and guarantees in this model are identified and it is described how they interact. This model is also used to analyse and compare existing implementations and their trust assumptions. The last chapter of the theoretical part is concerned with a protocol for UniBoard, which is our implementation of a bulletin board service. This protocol does not only tackle the guarantees but also so touches organizational and operational problems that might occur when running the service. The implementation part features two implementations. First UniBoard, which is an implementation of the already mentioned protocol and focuses on a modular design to be easy adaptable. Secondly parts of the implementation of UniVote, which is an e-voting application used to run student council elections at various universities in Switzerland, are discussed.

Jury:

- Prof. Dr. Philippe Cudré-Mauroux, University of Fribourg (jury president),
- Prof. Dr. Ulrich Ultes-Nitsche, University of Fribourg (thesis supervisor),
- Prof. Dr. Rolf Haenni, Bern University of Applied Sciences (thesis supervisor),
- Prof. Dr. Bryan Ford, Swiss Federal Institute of Technology in Lausanne EPFL