Verifiable Student Board Elections with UniVote

Eric Dubuis and Rolf Haenni
Research Institute for Security in the Information Society
Bern University of Applied Sciences
CH-2501-Biel, Switzerland

UniVote is a verifiable Internet voting system for student board elections at Swiss universities. It supports complex elections with open party-lists and cumulation of candidates. From the voter's perspective, it is a web application that runs in the web browser. The user interface has been designed for making the vote casting process as simple as possible even for the most complex elections, but the needs of voters with disabilities has not yet been addressed properly. To participate at UniVote elections, voters are required to go through a one-time registration process, in which the standard university login process is used for authentication. Currently, an affiliation to a Swiss university is therefore a prerequisite for using UniVote.

To provide verifiability, UniVote publishes all the election data on a public bulletin board. Upon registration, voters create an private Schnorr signature key, which they use for signing the encrypted votes. Prior the an election, the corresponding public keys are mixed in a mix network to allow anonymous vote casting. The encryption key is shared among multiple parties to protect the secrecy of the vote at all times. At the end of the voting period, the votes a mixed in another mix network and jointly decrypted by the parties holding the shares of the decryption key. All computational steps are accompanied with corresponding non-interactive zero-knowledge proofs to demonstrate adherence to the protocol. Voters receive a signed receipt of their vote cast, which they can use for individual verification and in case of a complaint.

A verification software called *VoteVerifier* has been developed independently by two students. The software retrieves all the election data from the public bulletin board and performs a total number of 60 different cryptographic checks. These checks are derived from the system specification and implemented accordingly. At the moment, some of the checks fail due to some deviations of the current UniVote implementation from the specification. The code base of VoteVerifier is completely disjoint from UniVote.

The current version of UniVote is implemented using technologies such as Java EE (EJB, JPA, JAXB) and web services (SOAP). On the client side, UniVote comes as a singe-page web application (HTML, CSS, JavaScript, JQuery), which uses AJAX technology for communicating to the servers. For the cryptographic computations, a Java library called *UniCrypt* has been developed as an independent sub-project. The source code of the whole project is publicly available.

In spring 2013, student board elections have been conducted at the University of Bern, the Bern University of applied sciences, and the University of Zürich. The accumulated size of the electorate is approximately 43'000. There was average turnout of roughly 10%. Most voters provided a positive feedback regarding the usability and the perceived security. Further elections are planned at the universities of Lucerne and Basel in the second half of 2013. The student association of the University of Zürich is furthermore planning to use UniVote for the signature collecting process of student initiatives and to run corresponding referendums.

Links

- Official UniVote web page: https://www.univote.ch
- Project web page: http://e-voting.bfh.ch/projects/univote/
- System specification: http://e-voting.bfh.ch/app/download/5874743461/specification.pdf
- Source code: https://wali.bfh.ch
- VoteVerfier: https://github.com/EVGStudents/VoteVerifier

References

- R. Haenni and O. Spycher. Secure internet voting on limited devices with anonymized DSA public keys. In *EVT/WOTE'11, Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, San Francisco, USA, 2011.
- E. Dubuis, S. Fischli, R. Haenni, S. Hauser, R. E. Koenig, P. Locher, J. Ritter, and P. von Bergen. Verifizierbare Internet-Wahlen an Schweizer Hochschulen mit UniVote. In *INFORMATIK'13, 43. Jahrestagung der Gesellschaft für Informatik*, Koblenz, Germany, 2013.