eTegrity: an electronic voter-verifiable voting system
Alex Florescu
The George Washington University
School of Engineering and Applied Science
Computer Science Department

Collaborators:
David Chaum, Mridul Nandi, Stefan Popoveniuc, Jan Rubio, Poorvi L. Vora
(adviser)

Audio files recorded by:
Tudor Petre Marin (producing, editing)
Andreas Aron (voice)

Research Sponsored by NSF-CNS-0831149

Summary:

eTegrity is a completely electronic voting system that allows voters to perform checks of the election integrity without requiring them to trust either the election authority or the voting machines used for casting the ballot. The novelty is in the approach of using a second computing device to assist the voter in auditing the election.

The protocol uses the cryptographic back-end of Scantegrity — the first voter-verifiable voting scheme to ever be used in a real election, in Takoma Park, Maryland in November 2009 — but while Scantegrity is based on paper ballots, eTegrity performs the entire process electronically. The main motivation for creating a paperless scheme is to make it possible to add accessible interfaces, so that it could be used by voters with disabilities who would otherwise not be able to vote unassisted. To demonstrate this concept, eTegrity’s implementation also includes an audio interface for the voting machine.

An electronic verifiable voting scheme raises challenges that paper schemes do not. For example, checking the voting machine to ensure it records the votes as they were cast is a very important problem. For that, eTegrity uses an “assistant”, specifically a computing device the voter brings in and uses it to perform checks of the cryptographic functions that the voting machine has executed. This solution raises another problem itself, because, in order to preserve privacy, the computing device that the voter brings in must not be able to obtain the selections that the voter has made. The main theoretical challenge was designing the protocol to tackle these issues, while also maintaining usability.
As far as implementation, the project consists of two distinct applications, one running on the voting machine and the other running on the “assistant” (in our case an Android-based smartphone). A big implementation challenge was making the two devices communicate over a USB cable connection and having them perform several checks on each other. The assistant verifies integrity by ensuring that the voting machine performs correct encryptions and the voting machines preserves voter privacy by preventing the assistant from finding out the actual votes. Another important challenge in the implementation was adapting Scantegrity’s functionality to the requirements needed for an electronic protocol, considering that Scantegrity was designed for papers ballots and not for a live electronic election system. In terms of usability, the software on the voting machine has both an audio and a visual interface that run synchronously, while the smartphone application only has a visual interface.

The voter, using these two devices as instructed, can either choose to cast a ballot and then check the confirmation codes (encryptions of the votes) to ensure that the votes were counted correctly or can choose to audit the election system, in order to check that the votes are encrypted correctly. Since the voting machine cannot know what the voter will choose, it must serve correct information or risk being caught with a high probability.

The eTegrity protocol and implementation represent significant research work and a conference paper is currently in preparation, as well as an open-source release being planned for June 2010.