The KOA Remote Voting System : A Summary of Work To-Date

Systems Research Group
School of Computer Science and Informatics
UCD Dublin Belfield, Dublin 4, Ireland
http://www.ucd.ie/csi

The KOA Remote Voting System

- Remote internet voting incorporates many of the core challenges of trusted global computing.
- Kiezen op Afstand (KOA) is a Free Software, remote voting system originally developed for the Dutch government.

Formal Specification and Verification

- In addition to being Open Source, KOA is also partially formally specified and verified.
- The vote counting system was formally verified using JML and ESC/Java2.
- The Irish vote counting system has since been specified using JML.

Internet Voting in the Netherlands

- The elections to the European Parliament of June 2004 allowed remote voting via the internet and telephone.
- The existing remote voting system was based upon postal ballots.

The Remote Voting Process

- When a citizen registers to use KOA, the voter chooses his or her own personal access code.
- Each candidate is assigned a large set of unique random numbers, and exactly one of those numbers is given to each voter.

Vote Verifiable Audit Trail (VVAT)

- When a voter is finished, a transaction code is provided.
- This code can later be used to check in a published list that the voter's choices were included correctly in the final tally.

Network Security

- Communication with the voting web site is secured with SSL.
- Each vote is encrypted by a symmetric key per voter and a public key of the voting authority.

Open Source Release of KOA

- In July 2004, the Dutch Government released the majority of the source code for the KOA system under the GNU General Public Licence (GPL) making it the first Open Source internet voting system in the world.

Formal Specifications for KOA

- The tally application for the Dutch system consists of 30 classes, which can be grouped into three categories:
- the data structures,
- the user interface, and
- the tasks.

Specifying Data Structures

- The data structure classes form an excellent opportunity to write JML specifications.
- Typical concepts from the domain of voting, such as candidate, district and municipality can be modeled with detailed JML specifications.

Specifying Tasks

- The different tasks associated with counting votes were mapped to individual Java classes.
- After successful completion of a task, the application state is changed. A task can only be started if the application is in an appropriate state.

Life Cycle Model

- This life-cycle model can be specified in JML using invariants and constraints, essentially stating that on successful completion of the application, the application went from ‘initial state’ to ‘votes counted state’.

Irish Vote Counting System

- The Dutch Voting system is list based
- Ireland uses Proportional Representation with a Single Transferable Vote (PR-STV)

Irish Vote Counting Specification

- 39 formal assertions were identified in the Count Rules published by the Irish Government.
- Each assertion was expressed in JML and identified by a Javadoc comment.
- A state machine was specified so as to link the assertions together.

Ongoing and Future Work

- The security properties, including a functional specification, for a MIDP-based remote voting application are in the process of being defined.
- We would be interested in collaborating to formally specify and verify a voting subsystem for use in American elections