Project Description:

Online Elections

Application Scenario

Imagine the following scenario: the Student Union (pf) wishes to introduce online voting to choose the recipient of the prestigious “Golden Pillow Award”, which is given to the most boring lecturer in four different categories: most boring lecture, most boring exercise (“regneøvelse”), most boring lab (“laboratorie øvelse”), and most boring use of new media, including the web. The Student Union nominates 2 - 5 lecturers in each category and all registered students should be allowed to cast the ballots.

For fear of retribution, from losing lecturers, the voting mechanism must prevent linkability between the identity of the person voting and any particular vote. It is also a requirement that only students at DTU are allowed to vote and that each student is only allowed one vote. Tabulation of votes should be done in public, e.g., all votes should be listed on a web-page, in order to allow public scrutiny of the election result.

Project Definition

Design, and evaluate a fair online voting system, that addresses the issues presented by the scenario outlined above. Issues that *must* be addressed are:

- Authentication of registered students: Is Campus Net authentication sufficient or should new infrastructures, such as public key infrastructures (PKI) or smart card be considered.
- Risk analysis: What assets are at stake?
- Threat model; you should explicitly state what threats your system has been designed to handle, e.g., ballot box stuffing, vote selling, etc.
- Security: Make sure that your system protects against the security issues raised in the threat model, and clearly document the threats that you do not protect against.