Homework9

SECURE VOTING

This document describes the voting process using an election terminal located in polling stations, and how security issues are handled.

PROCESS

A set of tokens was generated for each election district. These tokens are character strings that encode both election ID and election district.

Having entered a polling station in their home district, voters are asked for their ID card by a canvasser. The canvassers mark the voter's name as 'has elected' and the voter is allowed to draw one token from a ballot. Canvassers control that exactly one token was taken.

The voter is granted physical access to the voting terminal and unlocks it by entering the token code. The token is transmitted to the database and is disabled for any future use.

The election terminal shows the date and district of this election, as well as all possible first votes and second votes. After submitting of the vote, the terminal is locked again. The voter is than asked to leave the polling station.

PROTECTION AGAINST MANIPULATION

BRUTE-FORCE-ATTACKS*:* As the voting terminals are located in polling stations and are therefore under the control of the canvassers, we consider it sufficient to handle brute force attacks by timeout measures. After inserting an illegal token code (wrong election Id or wrong district encoded, or completely nonsense) the terminals front page is locked for several seconds. If this happens three times, the terminal is blocked and the user is informed that only the local election supervisor can unlock it again with a master code.

MULTIPLE VOTES WITH SAME TOKEN: it is impossible to submit more than one vote with one token. All used tokens are stored in the database and their ability to unlock the terminal is disabled once they were used.

SQL INJECTION: The only text input in this voting process is the authentication token. This input is transferred to a framework, that checks if it is valid and than opens the connection to the database. Therefore SQL injections are avoided, as the input is made before any connection with the database. The database connection is established after the token was validated. In addition, the only data transferred to the database are the IDs of voted candidate and party.

UNAUTHORIZED VOTERS: It is not possible for any unauthorized persons to vote, as the tokens to unlock the terminals are only given to persons who's ID was checked by a canvasser. Access to the voting terminals is exclusively granted after successful check of identity and token passing.

PRIVACY PROTECTION

Tokens are only related to the election and the district, and are not related to any persons.
Even though someone might have observed which token a single voter has drawn from the ballot, it is not possible for him to conclude a single vote from the use of that certain token. This is granted, because the token is only used to unlock the voting terminal and not for database access.