IPSA World Congress
RC10 Electronic democracy
Monday, July 13. and Tuesday July 14. 2009
Santiago de Chile

Vulnerability Analysis of Three Remote Voting Procedures

Enguehard, Chantal - LINA, France, chantal.enguehard@univ-nantes.fr

We analyze three remote voting procedures that are used in uncontrolled environments: postal voting, Internet voting and hybrid voting (e-counting of votes that have been mailed). For each of these modes we define a model inspired by a widely used application that can be regarded as representative of the general practices.

— Internet voting procedure used in the canton of Geneva in 2007.

— postal voting procedure used in the canton of Geneva in 2007.

— hybrid voting procedure used for the elections of the "Comité National de la Recherche Scientifique" in France in 2008. Then we extrapolate phases that are common to these three voting methods. We evaluate how the three procedures meet the criteria of a democratic vote (confidentiality, anonymity, transparency, unity,sincerity), distinguishing attacks against the safety and violations of reliability. Each vulnerability is quantified by three parameters:

— The magnitude of a fraud or malfunction will be defined as the proportion of votes potentially affected by the fraud or malfunction.

— The difficulty of a fraud or malfunction will be defined as a fuzzy estimation of the probability of exploiting the vulnerability. In the case of a problem of technical reliability, it will provide an estimation of the likelihood of failure. For a fraud it will provide a measure of the complexity of the conditions which must exist in order for the fraud to be perpetrated successfully.

— The visibility of a fraud or malfunction is a measure of the level to which the consequences of the vulnerability are observable.

The study details the particular vulnerabilities of technical innovations that are still under experimentation: transmission of votes by Internet, multiple voting, centralized management of signature, e-counting, etc. Then it reviews the phases of each voting procedure and applies its evaluation method. It appears that, for several phases, automating (partly or entirely) the voting procedure and dematerializing the voting objects (ballots, ballot box, signing sheet), tends to substitute visible and reduced scope vulnerabilities with invisible and large scope vulnerabilities. Anonymity and sincerity are the most directly threatened aspects.