Key Concepts and Protocols in E-Voting

Rui F. L. Joaquim
CCISEL, Portugal

INTRODUCTION

With today's technology, it is possible to improve the decision support of our networked and virtual organizations. More specific we are talking about e-voting systems, namely Internet voting systems, which are a convenient way to express actors' will and/or opinion with all properties of traditional voting, such as: accuracy, democracy, privacy, and verifiability.

To look at e-voting systems only as a modern way to conduct political or private organizations' elections is diminutive of its potential. Whenever people's privacy is at stake e-voting expertise can come in hand. Examples of such scenarios are quality surveys to improve service quality, for instance banks and other private or public service entities; health related surveys, for instance sexual behavior survey to help in the creation of a plan to fight sexual transmitted diseases, and teaching quality surveys to help adapt classes' content to students' needs.

Currently, commercially-available e-voting solutions are mainly "black box software." Most sellers hide the problems of deploying an e-voting application just for the profit. It is necessary to be aware of the risks, difficulties, and problems raised by e-voting systems, as well as the current solutions. Only well-informed actors, who know the risks and guaranties of e-voting systems, can consciously decide on the use of e-voting systems to improve networked and virtual organizations. After all, we are talking about protecting our own privacy.

The main problems we face when designing an e-voting system occur exactly when we try to conciliate all voting properties, namely when we try to conciliate privacy with the other properties, for example how to conciliate privacy with verifiability. As a result of research in the field for the last 25 years, advanced cryptographic techniques such as blind signatures, mix-nets, and homomorphic ciphers were used to tackle such problems.

E-VOTING PROPERTIES

Before starting our discussion on e-voting it is useful to define the core properties of any voting system.

- **Accuracy:** A voting system is accurate if (1) it is not possible to alter a vote, (2) it is not possible to eliminate a valid vote from the final tally, and (3) it is not possible to include an invalid vote in the final tally.
- **Democracy:** A voting system is democratic if (1) it only allows eligible voters to vote, (2) it ensures that eligible voters vote only once, and (3) ensures the equality of knowledge, that is no partial results.
- **Privacy:** A voting system has the privacy property if (1) neither the voting authorities nor anyone else can link any ballot to the voter who cast it, and (2) no voter can prove that she voted in a particular way. An e-voting system that holds the condition (2) is also called receipt-free.
- **Verifiability:** A voting system is verifiable if it provides mechanisms to verify the correctness of the final tally.

THE RISKS OF E-VOTING

E-voting systems, namely Internet voting systems, still face several problems that prevent their widespread use today (California, 2000; Caltech-MIT, 2001; Cranor, 2001; Rivest, 2001; Rubin, 2002; Internet Policy Institute, 2001). The problems can be broadly divided in three main classes.

The first class includes security and fault tolerance problems inherited from the current Internet architecture. Vital services, such as DNS name resolution, can be tampered in order to mislead users into spoofing servers (Lioy, Maino, Marian, & Mazzocchi, 2000). IP routing mechanisms and protocols, managed by many different organizations, should deal with partial

communication outages. However, communication problems may still arise.

The second class includes problems that are specific to voting protocols. These problems derive from the assumptions of the protocols about the execution environment, namely:

- Client machines used by voters must be trusted, in order to act as trusted agents, which is hard to ensure in personal or multi-user computers with general-purpose commercial operation systems.
- Servers controlling the voting process do not (1) fail, (2) become unreachable or (3) pervert the voting protocol. The protocol perversion includes either not reacting properly to client requests or by trying to influence the election by acting as a voter.
- The voting protocol is not disturbed by communication problems or machine failures.

The third class includes problems that may be created by specific attacks against a voting protocol or a running election. Such attacks may try to get some useful outcome, by subverting the voting protocol, or simply ruin an election using denial of service (DoS) attacks against the participating machines or applications. Another kind of attack is the coercion of voters, which can happen if they can vote anywhere without supervision of electoral committees or other trustworthy agents.

E-VOTING DEPLOYMENT

There are two broad categories of Internet electronic voting systems that must be distinguished in any discussion about Internet voting (California, 2000). The difference is based on whether or not the election agency has full control over the client-side infrastructure and software used for voting.

- **Agency-controlled systems:** In these systems the actual computers and software used for voting, along with the networks to which they are immediately attached, and the physical environment of voting, are under the control of election officials (or their contractors, etc.) at all times.
- **Vote-from-anywhere systems:** These are systems intended to support voting from essentially any computer connected to the Internet anywhere in the world, for example from home, workplaces, schools, hotels, cybercafés, military installations, handheld appliances, and so on. In this case, the computers used as voting machines, the software on them, the networks to which they are immediately attached to and the physical surroundings are under the voter or third party control, but not under election officials control.

This distinction is fundamental. Systems that are not agency-controlled are difficult to secure against privacy hazards and security attacks that can arise from infection with malicious code or use of remote control software. Hence, for vote-from-anywhere systems it is substantially harder to achieve the same degrees of privacy and security of agency-controlled systems.

E-VOTING PROTOCOLS

To clarify the difficulties behind the development of e-voting systems follows an analysis of a simple voting protocol. In this simple protocol there is a voting authority (a software application) that is responsible to provide all the required properties (accuracy, democracy, privacy and verifiability). The simple voting protocol goes as follows: (1) a voter submits his ballot and identification (ID) to the voting authority; (2) the voting authority checks if the voter had already voted, if not it detaches the voter ID from the ballot and stores the ballot; (3) after the election close, the voting authority performs and publish the tally. At the first glance, this simple voting protocol works perfectly:

1. It protects the voter's privacy because the voter's ID is detached from the vote.
2. It is accurate because it only accepts votes after checking the identity of voters.
3. It is democratic because it only allows voters to vote once.
4. It is verifiable because the number of votes can be verified checking the number of correctly authenticated voters.

However, since the voting authority controls all the voting process, the one who controls the voting authority controls the election. Imagine that an entity **X** assumes the control of the voting authority software, either by exploring a vulnerability or by using a back