Internet Voting

Jordi Barrat i Esteve
Universitat Rovira i Virgili, Spain

Jordi Castellà-Roca
Universitat Rovira i Virgili, Spain

Josep Domingo-Ferrer
Universitat Rovira i Virgili, Spain

Josep Maria Reniu i Vilamala
Universitat de Barcelona, Spain

LEGAL REQUIREMENTS AND TECHNICAL SOLUTIONS

Internet voting denotes electronic voting (e-voting) systems that allow votes to be cast using the Internet. There are, however, other types of e-voting, like those based on optical ballots, those using computers without remote connection or those sent by phone (Kersting, 2004; Tula, 2005). All these systems can be used in political elections or private ones (binding examples of Internet voting: the 2000 Democratic primary in Arizona or an election in a chapter of the Institute of Electrical and Electronics Engineers in 1997).

Since Internet voting will be applied to a democratic framework, it should offer the same conditions required in traditional elections (Cranor, 1997; Gritzalis, 2003; Prosser, 2004; Trechsel, 2005). Therefore, the suffrage must be at least universal, free, equal, and anonymous (Mitrou, 2002).

Universal voting means that any person entitled to take part in an election should be able to cast a vote, and this in an authenticated manner to avoid impersonation by malicious third parties. An identification procedure is required to *authenticate* the voter, which entails more difficulties than the traditional exhibition of a paper identification (ID). There are at least three approaches to identifying the user of an Internet voting system: through something the user *knows*, the user *is* or the user *has* (Schneier, 1996).

Knowledge of a username and the corresponding password is the most widely used identification procedure ("something the user knows"). It has the advantage of simplicity and usability by a vast majority of users. Nevertheless, it has two major problems. This system makes vote selling very easy, since the voter only needs to send his or her username and password to the buyer. The second problem is the trade-off between security and usability. Reasonable security requires long passwords, which increases the risk of typing errors by voters.

The second approach is to use a public key infrastructure (PKI) (Adams, 1999). In this case, every voter has a key pair of a public-key cryptosystem ("something the user has") and that public key is certified, for instance, by the electoral authority. Since the voter is authenticated with his or her digital signature, this system requires a high protection of the voter's private key to avoid its unauthorized use by another citizen. A user-held cryptographic token or smart card is a good solution to store and operate the user's private key, because such hardware devices can be regarded as being tamperproof in most practical situations.

Biometric identification is the third approach to identification ("something the voter is"). It is the oldest form, because physical recognition is a biometric procedure used not only by humans but also by animals. The voter uses a device that obtains a biometric measurement; for instance, a fingerprint. This measurement or pattern is sent to the authentication service that verifies whether it matches the data previously stored about the voter. Important issues when using biometrics to authenticate a voter are: (1) to ensure that the biometric pattern came from the right person at the time of the verification; and (2) to ensure that the collected pattern matches the one stored for the voter (both patterns are likely to be slightly different due to measurement errors or variable biological conditions, so exact matching is unlikely even if both patterns correspond to the same person).

A combination of several of these three identification approaches is a sensible solution.

Freedom is another important requirement that may be jeopardized if the voter receives inaccurate information

Copyright © 2007, Idea Group Inc., distributing in print or electronic forms without written permission of IGI is prohibited.

during the voting procedure. It should be realized that information technologies greatly facilitate these kinds of inputs (i.e., political pop-ups). The voter should also receive complete, accurate and understandable information about the operation of the Internet voting system. Therefore, training campaigns and on-site assistance are required.

Internet voting, although it can also be used in controlled polling stations, is particularly attractive in a distributed scenario where the vote is allowed from any computer (i.e., from home). However, a distributed scenario entails additional dangers because it becomes possible to create a voting market, even a massive one, or to practice extortion upon some citizens (i.e., the employer upon employees). An Internet voting system not used in official polling stations can hardly eliminate these problems, and the solutions—criminal protection or a reduced application to some specific groups of voters (i.e., citizens living abroad)—may not be enough from a democratic point of view. This is, therefore, one of the key problems of Internet voting (Jefferson, 2004). However, some countries currently admit postal voting, which is subject to similar dangers; thus, Internet voting could also be acceptable to those countries. It is actually a social and cultural problem.

Additionally, freedom in voting requires adapting to the electoral tradition of each country. An electronic vote should not reduce or eliminate the idiosyncrasy of an electoral system. For instance, blank votes and especially null votes cannot always be analyzed as voter's errors. They are part of political behavior and, if they are allowed in traditional systems, they must also be included in any Internet voting procedure (Barrat, 2004).

An *equal* vote requires that voters and the candidates receive a correct treatment. Therefore, the voting system screen should be designed to avoid any discrimination. The order of the political parties and their logos must be carefully established. It is also compulsory to have a simultaneous exhibition of all candidates, since using multiple screens would benefit the first ones. On the other hand, the system must avoid multiple votes by the same voter and should not exclude a citizen legally entitled to vote. Finally, equality requires a system that can guarantee the accuracy of the results; in particular, it should be impossible to change or delete a vote already cast. While perfect accuracy will avoid these situations or, at least, will detect and solve them, a system is said to provide partial accuracy if it is able to detect manipulation, but unable to solve it.

The digital signature is a good tool to provide these accuracy and integrity properties (Fujioka, 1992). The digital signature yields proof that the vote has been cast by a valid voter and has not been modified afterwards. Specific storage devices that do not allow information to be erased once it has been written can also be used. Nonetheless, security properties of an Internet voting system are ultimately dependent on the software implementation; therefore, the security properties of a system must be auditable (*vid. infra*).

The *anonymity* of the vote means that nobody, not even the electoral board, can link the content of one vote with the person who cast it. The system should also avoid the disclosure of partial results. The traditional procedure achieves these goals in a very simple way: a ballot (with or without envelope) is inserted into a transparent urn that can be controlled by any voter until the final tally. An Internet voting system cannot offer a similar procedure, since anonymity depends on the software source code and a citizen without technical knowledge cannot check it.

The anonymity of the vote and the secrecy of the intermediate results are usually assured by the encryption of the vote with the public key of the electoral authority (Benaloh, 1986; Chaum, 1988). However, the private key used to decrypt the votes protected with the public key is a very sensitive piece of information. It is not desirable that this key be possessed by just one person because that person can be an easy target for coercion. A usual strategy is to split the knowledge of the key between the members of the electoral board using a cryptographic threshold scheme that requires a pre-set number of board members to recover the private key (Shamir, 1979). If the number of co-operating board members is less than the threshold previously fixed, they do not obtain any useful information about the private key.

On the other hand, there are two basic methods to guarantee privacy and anonymity in an electoral procedure: mixing (Chaum, 1981) and homomorphic encryption (Benaloh, 1986).

In the first one, the voter obtains an authorization token issued by an electoral authority. There are several methods for obtaining the token anonymously, so that the election authority cannot later link the token with a particular voter (Sako, 1995; Nurmi, 1991; Fujioka, 1992). In the second step, the voter sends his or her vote and the authorization token using an anonymous channel implemented with a set of servers—"mixing servers": each server receives the votes, permutes their order and re-encrypts and sends them to the next one. Once the last mixing server has sent the votes the tally process begins. Every vote is decrypted and the server verifies that the authorization token is valid. These mixing server operations are complex and current research focuses on obtaining a mixing method that can be efficiently and universally verified.

In the homomorphic protocol, the voter encrypts his or her vote and computes a proof that demonstrates the correct construction of the vote. The proof does not

3 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/internet-voting/11644

Related Content

A Historical Perspective of the Development of E-Gov in Brazil
Alexandre F. Barbosa, Álvaro Junqueira, Eduardo H. Dinizand Otávio Prado (2010). *Systems Thinking and E-Participation: ICT in the Governance of Society (pp. 246-259).*
www.irma-international.org/chapter/historical-perspective-development-gov-brazil/40466

Economic African Development in the Context of FinTech
Youssra Ben Romdhane, Sahar Loukiland Souhaila Kammoun (2020). *Employing Recent Technologies for Improved Digital Governance (pp. 273-289).*
www.irma-international.org/chapter/economic-african-development-in-the-context-of-fintech/245986

Acceptability of ATM and Transit Applications Embedded in Multipurpose Smart Identity Card: An Exploratory Study in Malaysia
Paul H.P. Yeowand W.H. Loo (2009). *International Journal of Electronic Government Research (pp. 37-56).*
www.irma-international.org/article/acceptability-atm-transit-applications-embedded/2070

Open Social Innovation
Teresa Cristina Monteiro Martinsand Paulo Henrique de Souza Bermejo (2015). *Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services (pp. 144-163).*
www.irma-international.org/chapter/open-social-innovation/121319

Gender and E-Government Adoption in Spain
Ramón Rufín Moreno, Cayetano Medina Molina, Juan Carlos Sánchez Figueroaand Manuel Rey Moreno (2013). *International Journal of Electronic Government Research (pp. 23-42).*
www.irma-international.org/article/gender-and-e-government-adoption-in-spain/95103