Chapter 45
Electronic Voting by Means of Digital Terrestrial Television: The Infrastructure, Security Issues and a Real Test-Bed

Roberto Caldelli
University of Florence, Italy

Francesco Filippini
University of Florence, Italy

Rudy Becarelli
University of Florence, Italy

Francesco Picchioni
University of Florence, Italy

Riccardo Giorgetti
University of Florence, Italy

ABSTRACT

In this paper a Digital Terrestrial Television (DTT) based voting system is presented. This electronic voting technology allows disabled users to cast their vote from home by using common well-known devices. The needed equipment are a TV set, a Set Top Box (STB) with its remote control and a telephone line. The complete infrastructure consists of an MHP (Multimedia Home Platform) application that acts as a client application, a server application that acts as a network/counting server for e-voting, and a security protocol based on asymmetric key encryption to ensure authentication and secrecy of the vote. The MHP application is broadcasted by a certified (e.g., national) TV channel that grants its originality. The user needs a smart card issued by a national authority and to sign the encrypted ballot. The voter can browse the application by acting on the STB remote control. The server application is in charge to verify user identity, to gather and store user's encrypted ballots and finally to count votes. The communication between the client application and the server takes place by means of a secured channel (using HTTPS) while the voting operations are secured with the help of asymmetric keys encryption.

DOI: 10.4018/978-1-4666-4422-9.ch045

INTRODUCTION

Electronic, mechanical, or electromechanical voting are nowadays form of voting commonly accepted in various countries worldwide. Despite of this diffusion, these voting techniques have been always criticized for many reasons. Typical critics are related to the possibility, for the voter, to audit his vote or have some kind of control on the underlying mechanism during the polling phase that is when the vote is cast. This kind of frights arise naturally from the intrinsic complexity and/or from the opacity of the mechanism itself and can be amplified by a justified sense of caution. These critics highlight that one of the most important open issues is security and in particular how to achieve or, eventually, increase it with respect to a traditional voting scenario. Electronic voting can, besides, enhance the accessibility to vote even for people living outside the country of origin or for disabled persons. Electronic voting, that is widely exploited, offers mainly two different approaches to solve both security and accessibility issues. The first approach aims to substitute traditional voting form in the polling stations with electronic machines trying to match the requirements for accessibility and security. The second tries to solve the accessibility issue by making people vote through web based or broadcasted applications, not disregarding the security of the communication channel that must be used in this case. Electronic voting machines in polling stations, named DRE (Direct Recording Electronic) voting systems (Federal Election Commision, 2001)(Federal Election Commision, 2001a), have been widely used especially after US presidential elections in 2000 when mechanical punching machines led to a large number of invalid ballots. Actually, despite of the confidence given by citizens to such a solution, DRE machines are very sensitive to various kind of attacks, as detailed in (Fisher & Coleman, 2005)(Kohno et al., 2007). In order to improve the security of DREs in terms of capability of performing an audit by the user, secrecy of vote, and relative independence from technical flaws the receipt approach has been proposed. As explained in (Chaum et al., 2008)(Chaum, 2004)(Essex et al., 2007) (Garera & Rubin, 2007) (Chaum et al., 2008), the central idea is to give the user an encrypted receipt which can be used to audit the vote as an evidence that the vote has been cast and that can be seen like the ballot itself, since the user's choice is encrypted. Typically these systems, implemented as electronic or manual, give as a result of the voting operation two distinct ballots. After the voting phase (this is part of the security mechanism) the user is asked to destroy one of these ballot, chosen by himself, and scan the other one. The scanned ballots are sent to a server that acts like a ballot repository. Since both the ballots are encrypted and only the combination of the two can give some chance of recovering the vote, at the end of the operation the voter owns an encrypted receipt. The actual ballot is readable only with the help of some codes owned by the trusted authority that controls the voting operation (e.g., the Ministry of Internal Affairs). To allow the user to audit his vote, every encrypted ballot is identified by a readable unique number. The number, that is decoupled from the user's identity, can be used to audit the ballot via web with the help of a specific web application.

Recently electronic voting has proposed a new approach based on web applications allowing user to vote from worldwide. One of the first experiment in this direction has been SERVE (Secure Electronic Registration and Voting Experiment) (Jefferson et al., 2007a), a web based application developed for military personnel deployed overseas. Its security is mostly based upon asymmetric key encryption and HTTPS connection. An analysis of possible security flaws can be read in (Jefferson et al., 2007). Other similar systems have been developed starting from the SERVE experience, as for the Estonian e-voting system used during political elections in 2005 (Mägi, 2007). The SERVE security architecture and the Estonian experiment have been used as a reference