Remote E-Voting Using the Smart Card Web Server

Sheila Cobourne, Smart Card Centre, Information Security Group, Royal Holloway, University of London, Egham, UK
Lazaros Kyrillidis, Smart Card Centre, Information Security Group, Royal Holloway, University of London, Egham, UK
Keith Mayes, Smart Card Centre, Information Security Group, Royal Holloway, University of London, Egham, UK
Konstantinos Markantonakis, Smart Card Centre, Information Security Group, Royal Holloway, University of London, Egham, UK

ABSTRACT

Voting in elections is the basis of democracy, but voting at polling stations may not be possible for all citizens. Remote (Internet) e-voting uses the voter’s own equipment to cast votes, but is potentially vulnerable to many common attacks, which affect the election’s integrity. Security can be improved by distributing vote processing over many web servers installed in tamper-resistant, secure environments, using the Smart Card Web Server (SCWS) on a mobile phone Subscriber Identity Module (SIM). A generic voting model is proposed, using a SIM/SCWS voting application with standardised Mobile Network Operator (MNO) management procedures to process the votes cast. E-voting systems Prêt à Votter and Estonian I-voting are used to illustrate the generic model. As the SCWS voting application is used in a distributed processing architecture, e-voting security is enhanced: to compromise an election, an attacker must target many individual mobile devices, rather than a centralised web server.

Keywords: Estonian I-Voting, M-Voting, Mobile Communication, Phone, Prêt à Votter, Remote E-Voting, Smart Card Web Server, Subscriber Identity Module (SIM) Card

INTRODUCTION

Voting in elections is generally regarded as a fundamental democratic right, but it can be a challenge to engage citizens and encourage them to vote. Participation in the democratic process could be improved by using remote e-voting systems, where a voter uses their own computer or mobile device to cast votes over the Internet. Examples of practical implementations of remote e-voting include elections in Estonia (Estonian National Electoral Committee, n.d.) and Switzerland (Geneva State Chancellery, n.d.).

The fundamental requirements for any voting system are that votes should be recorded as cast, counted as recorded and not linked to a specific voter. Only eligible voters should be allowed to vote, and they can only cast one vote each (Ryan, Bismark, Heather, Schneider,

DOI: 10.4018/ijsse.2014010103
Some e-voting systems are designed to address these requirements in the controlled environment of an election poll-site. Examples include fully electronic systems such as Votebox (Sandler, Derr, & Wallach, 2008), Direct Recording Electronic (DRE) machines (Appel et al., 2009; Kohno, Stubblefield, Rubin, & Wallach, 2004); and paper-based ballots such as Prêt à Voter (Xia et al., 2007) and the Scratch Card voting system (Randell & Ryan, 2006).

Remote e-voting systems, however, have to operate in unsupervised environments, leading to opportunities for denial of service and technical attacks on the voting infrastructure. For example, the voter’s equipment could be infected with malware that tampers with the vote, or a Voting Authority (VA)’s centralised web-servers could be attacked, as seen in the 2010 Washington D.C. election (Wolchok, Wustrow, Isabel, & Halderman, 2012) and the 2012 Canadian New Democratic Party Elections (Payton, 2012). These attacks can seriously undermine the credibility of an election. In the Washington D.C. case, the e-voting system was broken into within 48 hours of it becoming available, and by taking control of the election server, the attackers “changed every vote and revealed almost every secret ballot” (Wolchok et al., 2012). Coercion and vote-buying are also problems for remote e-voting. Anti-coercion measures are included in some e-voting systems e.g. Civitas (Clarkson, Chong, & Myers, 2008), but some schemes are specifically designed for use in low-coercion elections, such as Helios (Adida, 2008). Some e-voting schemes have been implemented on mobile devices: for example, SEAS (Baiardi et al., 2005) was implemented on a mobile phone and formally analysed by Campanelli et al. (2008).

Although many e-voting processes can be cryptographically protected to ensure the integrity and confidentiality of the votes cast, Rivest (2001) identified a critical problem with remote implementations, i.e. “interfacing the voter to the cryptography”. Security weaknesses in hardware, operating systems and software mean that equipment cannot be trusted. This is known as “the secure platform problem”. Several methods to address this have been proposed (Oppliger, 2002). One approach is code voting, when voting authorisation codes are sent to voters before the election, via a second channel such as the postal service: see (Helbach & Schwenk, 2007; Randell & Ryan, 2006; Ryan & Teague, 2009) for examples.

Two methods could be used to make attacking a remote e-voting system less attractive. Firstly, installing vote processing in a trusted tamper-resistant environment that can only be accessed by authorised parties will reduce the opportunity for malicious modifications to the voting application. Secondly, distributing vote processing over a large number of web servers will mean that an attacker must target multiple sites to be successful. The most ubiquitous tamper-resistant security token available is the mobile phone SIM. Generally, the term SIM is used to describe a type of smart card that consists of the Universal Integrated Circuit Card (UICC) and application software that allows telecommunication access called the USIM (for 3G networks) or SIM (for 2G networks) (Mayes & Markantonakis, 2007). Here the term “SIM” will be used generically to represent the smart card used with a mobile phone. A SIM equipped with a Smart Card Web Server (SCWS) (OMA, 2008a; OMA, 2008b) has web server functionality in the SIM environment, so a distributed vote processing application can be installed and run in a tamper-resistant environment. The use of the SIM means that the vote processing application is not accessible to an adversary who attacks the mobile phone platform.

A mobile phone SIM is a restricted processing platform, so a voting application cannot necessarily perform all required e-voting system functions. It can provide a “front-end” input method to more sophisticated cryptographic e-voting systems which do have the required resources. This work proposes a generic SCWS-based voting procedure that can be used with existing e-voting systems to provide a complete voting solution. As examples, the SCWS approach will be shown with the e-voting systems Prêt à Voter (PAV) (Ryan et al., 2009) and Estonian I-voting (Estonian National Electoral
Using Model-Driven Architecture Principles to Generate Applications based on Interconnecting Smart Objects and Sensors
Cristian González García and Jordán Pascual Espada (2014). Advances and Applications in Model-Driven Engineering (pp. 73-87).
www.igi-global.com/chapter/using-model-driven-architecture-principles/78611?camid=4v1a

Formal Semantics of Dynamic Constraints and Derivation Rules in ORM
Herman Balsters and Terry Halpin (2016). International Journal of Information System Modeling and Design (pp. 31-47).
www.igi-global.com/article/formal-semantics-of-dynamic-constraints-and-derivation-rules-in-orm/162695?camid=4v1a