Chapter 18

Komminist Weldemariam
Fondazione Bruno Kessler, Italy

Adolfo Villafiorita
Fondazione Bruno Kessler, Italy

ABSTRACT

In this chapter, first the authors discuss the current trends in the usage of formal techniques in the development of e-voting systems. They then present their experiences on their usage to specify and verify the behaviors of one of the currently deployed e-voting systems, using formal techniques and verification against a subset of critical security properties that the system should meet. The authors also specify attacks that have been shown to successfully compromise the system. The attack information is used to extend the original specification of the system and derive what the authors call the extended model. This work is a step towards fostering open specification and the (partial) verification of a voting machine. The specification and verification was intended as a learning process where formal techniques were used to improve the current development of e-voting systems.

INTRODUCTION

Modern electronic voting (e-voting) system started in the mid 90’s as a system to support traditional voting in many ways and has since then evolved into a full-fledged system attempting to ensure safe and secure elections. This has been made possible somehow by the introduction of a number of mechanisms such as the introduction of the direct recording electronic, DRE, (Cranor, 1996; Mercuri & Camp, 2004). These mechanisms are the basis to improve elections by over-performing of traditional voting systems, such as to allow accessibility and prevention of voter mistakes,
let the visually impaired vote without assistance, and vastly simplify the ballot management using some kinds of memory cards instead of paper.

However, the effect of widespread deployment of e-voting systems is that the security perimeter of a typical modern government has also changed markedly. This is evident from much increased interest over the last few years in the study of the development process and security of e-voting systems. Numerous recent security studies revealed that most currently deployed DRE-based e-voting systems share critical failures in their design and implementation, which render their technical and procedural controls insufficiency to guarantee trustworthy voting. One of the main reasons for this is that the development of existing e-voting systems are directed almost exclusively at large scale known engineering disciplines and consequently a niche too small to drive significant adoption of e-voting technology into our democracy. Other factors contribute to make e-voting systems a less adopted for critical elections. For example, existing methodology for requirements structuring mostly provide high-level principles and recommendations for e-voting systems development, see, e.g., (McGaley, 2008; Volkamer, 2009). In one hand, this is due to the sophisticated nature of the requirements for e-voting systems. On the other hand, there is little or no tool to support the management and structuring of these requirements. Obviously, this would create further difficulty in realizing the links between legal regulations and technical requirements, as well as in realizing the requirements during development process.

Today, in fact, we now have a much better understanding of the issues that pose the development of a trustworthy e-voting system. However, it is not clear that which development process that we require to follow, that how requirements can be allocated during the execution and monitoring of the actual election, and that how incidents occurred during the election should be analyzed after election and then incorporating the analysis results in the next development cycle. Additionally, as noted in (Oostveen & den Besselaar, 2004; Gardner et al., 2007), we have a long way to go in terms of providing a mean through which we convince how individual vote is really recorded and stored. However, to tackle some of these issues, a range of development trends and technological solutions have been explored and proposed (Sastry et al., 2006; Paul & Tanenbaum, 2009). Several standards and requirements development strategies have also been introduced in the literature for the development of trustworthy e-voting systems (Bryans et al., 2006; Anane et al., 2007; McGaley, 2008; Volkamer, 2009). Works that evaluate the security of e-voting systems have also been discussed, e.g., in (Kohno et al., 2004; Ansari et al., 2008; Aviv et al., 2008; Balzarotti et al., 2010; Wolchok et al., 2010).

We believe that the security of e-voting systems can be improved through a multidisciplinary approach that requires know-how in business process modeling (for understanding the context of elections), formal methods (for detailed formal analysis of critical security and safety requirements about the system and its procedures), and system or security engineering (for the adoption of rigor secure-aware development process). This chapter, though, will focus on the usage of formal methods in the specification and verification of e-voting systems. Existing works in formal methods present specification and verification of e-voting systems at different level of abstractions. These works particularly aimed to demonstrate the feasibility of formal verification of voting machine logic, thereby providing a higher level of assurance on the security of the system.

In this chapter, we particularly discuss where formal methods can be incorporated in e-voting systems development process using our past experiences as evidence. We applied formal modeling techniques where we felt they would add rigor to the development and evaluation of an e-voting system named ProVotE (Villafiorita et. al, 2009). In this case, the usage of the formal methods was intended to improve the development process of the ProVotE e-voting system. In contrast, we
Related Content

An Exploration Regarding Issues in Insider Threat
www.igi-global.com/chapter/an-exploration-regarding-issues-in-insider-threat/173125?camid=4v1

A Novel OpenFlow-Based DDoS Flooding Attack Detection and Response Mechanism in Software-Defined Networking
www.igi-global.com/article/a-novel-openflow-based-ddos-flooding-attack-detection-and-response-mechanism-in-software-defined-networking/148301?camid=4v1a

Perceptions and Framing of Risk, Uncertainty, Loss, and Failure in Entrepreneurship

Securing the Internet in New Zealand: Threats and Solutions
Jairo A. Gutierrez (2000). Internet and Intranet Security Management: Risks and Solutions (pp. 24-37).
www.igi-global.com/chapter/securing-internet-new-zealand/24596?camid=4v1a