Chapter 4

A Holistic Framework for the Evaluation of Internet Voting Systems

Stephan Neumann
TU Darmstadt, Germany

Melanie Volkamer
TU Darmstadt, Germany

ABSTRACT

The foundations of democratic societies are elections. Due to their central importance to society, elections are bound to high legal standards, which are usually specified as election principles in national constitutions. To date, technological advance has reached elections, and Internet voting is a buzzword in the field of information technology. Many Internet voting systems and schemes have been proposed in research and some have even been used in legally binding elections. However, their underlying requirements are on the one hand often too closely linked to the specific technology and on the other hand mostly tailored to the scheme/system under investigation and therefore not connectable with election principles. This makes it difficult to compare different schemes/systems with each other, and correspondingly, it is difficult for election officials to select one of the proposed Internet voting schemes/systems for their own election setting. This chapter counters this artifact with two contributions, which are captured within an evaluation framework. First, based on the interdisciplinary method KORA, the authors derive constitutionally founded technical requirements. Second, they propose metrics to estimate the fulfillment of these requirements within concrete Internet voting systems. Given these contributions, the framework developed within this chapter supports election officials in making justified decisions about the selection and deployment of a specific Internet voting scheme/system.

DOI: 10.4018/978-1-4666-5820-2.ch004
INTRODUCTION

Elections build the basis of democratic societies and represent the exercise of popular sovereignty. The implementation of such a powerful means is therefore bound to high legal standards. Even though those standards might slightly differ depending on the specific national constitution and election type, all democratic states agree on three election principles namely universal, equal, and free according to the Universal Declaration of Human Rights (United Nations, 1948). Some states prescribe the deployment of even more election principles. For instance, the German Constitution anchors the principles of universal, equal, and free elections, but also requires the implementation of the secret, direct, and public nature principles.

With the rapid advance of modern communication technology elections have come into the focus of technical scientists; electronic voting has become a buzzword within the area of information and communication technology. The anticipated benefits of electronic voting are - amongst many others - the decrease of voter discrimination, the increase of voter turnout, the reduction of cost, and faster vote tallying. Starting with the seminal work by Chaum (1981), the challenge of voting over the Internet has been addressed by many researchers and many Internet voting schemes have been proposed to date, see for instance the works by Fujioka, Okamoto, and Ohta (1992), Juels, Catalano, and Jakobsson (2005), and Adida (2008). As opposed to purely theoretical considerations, several implementations of Internet voting schemes have found their way to practice and have been used for real-world elections, see for instance the presidential elections at the Université catholique de Louvain (Adida, de Marneffe, Pereira, & Quisquater, 2009) and the Estonian parliamentary elections (Maaten, 2005).

While the scientific literature often provides Internet voting schemes with proof (or at least strong evidence) for their security, the underlying security requirements are on the one hand too closely linked to the technology and on the other hand mostly tailored to the scheme under investigation. The same holds for other types of requirements such as functional and usability related requirements. Therefore, a legal evaluation of Internet voting systems and the resulting selection of adequate Internet voting systems with regard to the specific election setting seems hardly possible.

The goal of this work is to build a holistic evaluation framework that enables one to evaluate Internet voting systems according to the same requirements, i.e., the evaluation results for different Internet voting systems are comparable. Furthermore, the results are linked to election principles and thereby do not only cover security requirements. The evaluation of Internet voting systems according to this framework thereby leads to measurable outcomes, i.e., goes beyond existing approaches such as Common Criteria Protection Profiles which only allow statements about compliance or non-compliance of Internet voting systems and additionally only address security requirements.

In the remainder of this work, we first specify the target of evaluation, namely Internet voting systems. As election principles are too abstract to evaluate systems against, we deduced, in an interdisciplinary research project, a list of requirements that serve as basis for the evaluation of Internet voting systems. We shall emphasize that the focus of this work is on the German Constitution. However, we explain how to adapt this work for other legal settings. The subsequent section is dedicated to the derivation of metrics for the determined requirements. These metrics are based on an extensive literature review. We additionally account for the importance of scientific literature in the field of Internet voting by outlining mappings between the requirements and metrics derived within, and the system properties and attacks widely known in the technical literature. We thereafter review