Chapter 2

Analysis of Security and Cryptographic Approaches to Provide Secret and Verifiable Electronic Voting

Stephan Neumann
TU Darmstadt, Germany

Jurlind Budurushi
TU Darmstadt, Germany

Melanie Volkamer
TU Darmstadt, Germany

ABSTRACT

Electronic voting systems are inextricably bound to security and cryptographic techniques. Over the last decades, countless techniques have been proposed to face the dangers of electronic voting systems with mathematical precision. Certainly, the majority of these works address secrecy and verifiability. In this chapter, security and cryptographic techniques are analyzed with respect to those security properties that can be evaluated on the basis of these techniques: secrecy, fairness, integrity, and verifiability. Furthermore, the chapter discusses their adequacy to ensure further relevant properties like eligibility and uniqueness, and evaluates security and cryptographic techniques with respect to the costs that come along with their real-world application. The authors conclude the chapter with a summary of the evaluation results, which can serve as guideline for decision-makers.

INTRODUCTION

The history of elections reaches back to ancient Greece and ancient Rome where citizens elected public positions. The implementation of elections has changed over thousands of years from showing of hands to throwing stones and shards into buckets, up to filling paper ballots and throwing them into sealed urns. Since the 1960s, electronic systems are gaining the public interest due to the possible benefits of accurate, fast, and cheap elections. Early electronic voting systems were
implemented as voting machines, only since the 1990s, remote electronic voting systems enter the field and turn out to be a promising implementation of absentee voting. Throughout this chapter, we consider only remote electronic voting and use the term electronic voting interchangeably.

Electronic voting systems are inextricably bound to security and cryptographic (SnC) techniques to provide secret, fair, and verifiable elections as well as integrity. Note, SnC techniques considered throughout this work are detached from identification and authentication mechanisms, as this is an orthogonal research direction to this work. Looking back on more than three decades of research, there is a wide range of security and cryptographic techniques striving for secure electronic voting. These techniques are tailored towards special needs and different compromises are made among different properties. Unfortunately, the security model each of the security properties is based on is not specified clearly or is specified in different ways for different approaches. This makes it difficult to compare the different security and cryptographic techniques proposed for secure electronic voting and thus to decide which is appropriate for a special type of election. This gap is addressed within this chapter. Thereby, we support decision-makers in finding adequate SnC techniques to implement electronic voting with respect to their targeted electoral circumstances.

We focus our analysis on security and cryptographic techniques. Correspondingly, the focus is on those security properties which these techniques can already provide without combining them with identification and authentication techniques and without building the whole voting system. These are: secrecy, fairness, integrity, and verifiability. The concrete definitions of these security properties were derived within an interdisciplinary project between legal and technical scientists. These definitions are provided in this chapter. In addition, we developed a common modular security model allowing us to deduce the degree of fulfillment of these properties for concrete SnC techniques. This security model contains an exhaustive list of adversarial capabilities which were deduced from the literature. This security model is presented in this chapter. We, afterwards, select well known SnC techniques for electronic voting systems from the literature and evaluate them with respect to their security model. Moreover, we shortly discuss the SnC techniques’ adequacy to satisfy further security properties namely eligibility and uniqueness when combined with corresponding identification and authentication techniques, as well as the costs to apply these techniques within real-world applications.

Before diving into the main sections of this chapter, we added a background section. Here, we review the related work, provide an overview of the components involved in the electronic voting process, and the preliminaries required in the remainder of this work. We conclude the chapter with a summary of our work and point the reader to future research directions in the electronic voting community.

BACKGROUND

The first part of this section reviews related literature and shows where the present work is settled in the current state of the art on SnC techniques. In the second part, we outline components generally involved in the electronic voting process. Afterwards, we provide the preliminaries used throughout the analysis. More precisely, the preliminaries cover secret sharing techniques, encryption schemes, digital signature schemes, zero-knowledge proof systems, and the Benaloh challenge. The reader familiar with these preliminaries can safely skip these parts.

Related Work

In this subsection, we review comparative surveys and analyses of SnC techniques in electronic voting systems and settle our own contribution. In