Preface

Assuring the integrity of the outcome of an election and guaranteeing the secrecy of ballots forms the foundation of a healthy democracy. For conventional voting, using paper ballots and hand-counting, procedures have evolved over time that by and large are perceived to be trustworthy in providing these guarantees. However, with the dawn of the digital age there are increasing trends to move away from traditional ways of conducting elections to ones using digital technologies. The most extreme form of this is the conduct of elections over the Internet. Any such moves bring a host of new, unfamiliar and often severe threats. On the other hand, digital technology can bring significant benefits in terms of convenience, efficiency, etc. The challenge of ensuring that elections conducted electronically provide at least as much security as traditional ones, and ideally more, has been taken up in earnest by the cryptography and security communities over the past couple of decades or so.

In 2003, Springer published a book entitled *Secure Electronic Voting* (ed. Dimitris Gritzalis). The book features a collection of chapters authored by then active researchers in the field. It presented the latest trends, threats and the state-of-the-art technologies in electronic voting (e-voting) at the time of its publication.

A decade on, significant advances have been made both in theory and practice, and the landscape of the field has changed dramatically. On one hand, e-voting has been widely deployed in democratic countries around the world, e.g., USA, India, Brazil and Estonia. But on the other hand, e-voting has also become very controversial. Many deployed e-voting systems have been reported to contain serious security vulnerabilities. Consequently, their use has been discontinued in a number of countries, including the Netherlands, Ireland and Germany. One central concern with these (discontinued) e-voting systems is a lack of verifiability: namely, the lack of any means of verifying that votes have been correctly recorded and tallied. The need to address the verifiability problem has encouraged the development of several academic solutions to the problem of end-to-end (E2E) verifiable voting, and the resulting systems to move from theory to practice. The deployment of E2E voting systems in real-world elections is in fact considered one of the most significant developments in the field in the last decade.

This book aims to cover all the major developments in electronic voting, in particular, E2E voting systems, from 2003 (taking the story forward from the Gritzalis book) to present "real-world" settings. It covers three broad areas: new e-voting protocols, new attacks reported on e-voting and new developments in the real-world use of e-voting.

Both editors of this book are lead designers of two different E2E voting systems, called Prêt à Voter and DRE-i, both of which have been implemented and used in practical applications (detailed in Chapter 12 and 13, respectively). These two systems and others (Scantegrity, Helios and STAR-Vote, as detailed in Chapters 10, 11 and 14, respectively) are examples of the diversity in the field. While providing similar E2E verifiability properties, these various systems are designed using different techniques, have different trade-offs and are suitable for different election scenarios.

In the light of these many advances in both the theory and the practice of e-voting since 2003, we felt that the time was ripe to take stock of the state of the art and to identify the remaining challenges. We are delighted and honored to be joined in this task by many of the most prominent researchers in the field, with expertise ranging from the legal and regulatory aspects of e-voting to cryptography, computer science and engineering.

We should note that this book is not intended to argue in favor of or against e-voting, but to present a factual account of what is known about the e-voting capabilities and limitations, based on the authors' experience in designing, analyzing and deploying e-voting systems in real-world settings.

This book is divided into three parts. The first part looks at the general principles involved in designing a secure e-voting system and deploying it in practice. It consists of the following two chapters.

- In Chapter 1, Ronald Rivest, a professor at MIT and Madars Virza, a researcher at MIT revisit the notion of "software independence." This notion was first proposed by Ronald Rivest and John Wack in 2006, and since then has proved to be an invaluable guiding principle for designing secure voting systems.
- In Chapter 2, Ben Goldsmith, drawing on his over 20 years' work experience in the International Foundation for Electoral Systems (IFES), lays out detailed guidelines for trialling e-voting in national elections. Many failures in past e-voting trials were the result of a lack of careful planning and appropriate management; this chapter provides guidance as to how these pitfalls may be avoided in the future.

The second part looks at real-world implementations of e-voting, in particular in national elections. It consists of the following five chapters.

- In Chapter 3, Carlos Vegas and Jordi Barrat, researchers from the eVoting Legal Lab, present an overview of the current state of e-voting implementations worldwide. This chapter focuses on legal and sociopolitical issues in e-voting, and highlights the importance of three pillars for a successful e-voting deployment, namely: technical background, legal framework and a proactive society. Any weak point in these pillars may lead to the failure of the e-voting project.

- In Chapter 4, Siamak Shahandashti, an ERC research fellow at Newcastle University, reviews the electoral voting systems that have been used in real elections worldwide. While academic research on E2E verifiable voting often focuses on the simple first-past-the-post system, it is worth noting that there are a great variety of voting systems that are far more complex. Supporting all these systems in the electronic context with E2E verifiability presents significant challenges to researchers in the field.

- In Chapter 5, Kristian Gjøsteen, a professor at the Norwegian University of Science and Technology, gives an account of the Norgwegian e-voting trials in 2009 and 2011. This account is based on the author's experience of participating in these trials as a member of the steering group and as a consulting cryptographer for both trials.

- In Chapter 6, Dylan Clarke, an ERC research fellow at Newcastle University, and Tarvi Martens, the chief architect of the Estonian remote Internet voting system, describe the Estonian Internet voting system. Since the first pilot in 2005, Internet voting has been used for the whole country in three sets of local elections, two European Parliament elections and three parliamentary elections.

- In Chapter 7, Alex Halderman, an associate professor at the University of Michigan, reviews practical attacks on real-world e-voting systems, from poll-site DRE to online voting. This chapter is largely based on the author's personal involvement, as an independent security expert, in several research projects that uncovered serious vulnerabilities in e-voting systems deployed in real-world elections.

The third part of this book looks at E2E voting systems and their use in real-world applications. It consists of 7 chapters.

- In Chapter 8, Taha Ali and Judy Murray, researchers at Newcastle University, present a comprehensive overview of existing solutions to building end-to-end (E2E) verifiable voting systems for both polling-station-based and internet-based elections. This chapter also contains a discussion on the legal framework for e-voting, which should be considered when adopting any E2E voting system for national elections.

- In Chapter 9, Peter Hyun-Jeen Lee and Siamak Shahandashti, researchers at Newcastle University, review various attacks against E2E verifiable voting systems in the literature. While E2E verifiability can provide a theoretical guarantee of the tallying integrity, imprecise details in the specification of the technical system or the voting procedure may expose the system to unexpected attacks.

- In Chapter 10, researchers in the Scantegrity team, including Richard Carbak, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc, Ronald Rivest, Emily Shen, Alan Sherman, Poorvi Vora, John Wittrock, and Filip Zagórski, recount a decade-long research effort in designing an E2E verifiable system known as Scantegrity. The Scantegrity system was adopted in the municipal elections of Takoma Park, MD, USA, in 2009 and 2011.

- In Chapter 11, Olivier Pereira, a professor at the Université catholique de Louvain, describes a web-based E2E voting system called Helios. Helios was initially designed by Ben Adida in 2008 and later improved by Ben Adida, Olivier De Marneffe, Olivier Pereira and Jean-Jacques Quisquater in 2009. In 2009, Helios was used in the university presidential election at the Université catholique de Louvain (UCL), and since 2010, has been regularly used for elections in universities (Princeton, UCL), associations (International Association for Cryptologic Research, ACM) and private companies.

- In Chapter 12, Peter Ryan, a professor at the University of Luxembourg (and one of the editors of this book), and his colleagues in the Prêt à Voter research team, including Steve Schneider of University of Surrey and Vanessa Teague of University of Melbourne, describe the evolution of the Prêt à Voter E2E voting system. Since its inception in 2004, Prêt à Voter has gone through several improvements, culminating in 2014 with the system being adopted in the Victoria State election in Australia.

- In Chapter 13, Feng Hao, a reader at Newcastle University (and one of the editors of this book), describes a 10-year research journey that led to the design of an E2E voting system known as DRE-i. Differing from other E2E voting systems, DRE-i does not involve tallying authorities, hence the system is termed "self-enforcing." Since 2013, a web-based implementation of DRE-i has been used in the campus of Newcastle University to provide verifiable classroom voting applications.

- In Chapter 14, Dan Wallach, a professor at Rice University, and his colleagues in the STAR-vote team, including Susan Bell, Josh Benaloh, Michael Byrne, Dana DeBeauvoir, Bryce Eakin, Gail Fisher, Philip Kortum, Neal McBurnett, Julian Montoya, Michelle Parker, Olivier Pereira, Philip Stark and Michael Winn, introduce the STAR-vote, a Secure, Transparent Auditable, and Reliable Voting System. It is planned that STAR-vote will be used for the elections at Travis County, TX, USA, in 2018.

This book is part of the CRC Series in Security, Privacy and Trust. We thank Dr. Jianying Zhou, the series editor, and Mr. Ruijun He, the CRC editor for reviewing and approving our initial book proposal. We greatly appreciate Mr. Ruijun He for his kindly agreeing to our request to make the book open-access two years from the publication. This is a key reason that we were able to attract many prominent researchers in the field to contribute to this book project. We also thank Ms. Marsha Pronin, the project coordinator at CRC Press, for her assistance in helping us prepare for this book and her patience along the way.

Last but not least, we would like to express our sincere thanks to chapter authors who joined us in writing this book, for their invaluable contributions on not only writing their own chapters, but also peer-reviewing other chapters. We feel we have learned so much from them. As editors and authors, we enjoyed working on this book, and we hope the reader will find the book useful and enjoy reading it.

Feng Hao
Newcastle University

Peter Y. A. Ryan
University of Luxembourg