Foreword

Voting is a unique task with many distinctive challenges. Many modern voters shop online, bank online, communicate online and wonder why they can't vote online as well. But when bank customers make deposits they get receipts, they can check records of their balances and they have established processes for resolving disputes. Shoppers know whether or not the goods they've purchased have been received, and they can see what charges have been incurred. None of these tools are typically available to voters.

If a bank were to transpose deposits and withdrawals, customers would immediately notice and complain. If an online retailer were to mislabel its offerings and send red jackets to those who ordered blue ones and vice-versa, it would be inundated with returns from angry customers. But in an election, if the votes for two candidates or parties were switched, who would know? We hope that election officials and equipment vendors are honest and highly-competent and that they would not allow such errors to happen, but how can voters be sure? Even under the best of conditions, traditional election systems cannot provide voters with the kind of assurances they receive in their other endeavors.

One of the most difficult aspects of elections is their extraordinary trust and privacy requirements. Most security systems protect insiders from outsiders. When a credit card is transmitted to make an online purchase, the principal threats are from third-parties who might wish to compromise the privacy or the integrity of the transaction. In contrast, every participant in an election system is potentially malicious: individual voters may wish to see how others voted, to sell their own votes to others, to unduly alter the election tallies, or even to disrupt the election and keep it from concluding; dishonest election officials may seek to disenfranchise voters, to learn how individuals voted, or to report inaccurate tallies; and corrupt equipment vendors might want to perpetrate all forms of mischief. Perhaps worst of all, surprising collusions may compromise elections: voters and election officials may conspire to sell votes; a coercive employer may conspire with an equipment vendor to ensure

that employees are voting according to instructions; or observers may conspire with election officials to alter or discard votes.

Election officials should not know how individuals voted, and voters should not be able to show others how they voted. Indeed, the exceptional privacy requirement that voters be unable to reveal their votes – even if they desire to do so – makes voting especially difficult.

In the mid nineteenth century, the "Australian ballot" was introduced as a means of deterring coercion; today we take for granted this process of voting privately within a public environment where observers can enforce privacy, but it was a great innovation in its time. As elections have moved from paper to punch cards to lever-machines to electronic consoles and back – with many intermediate stops – the challenges of maintaining privacy and integrity have grown.

In the early 1980s, cryptographers began to propose new election designs with new properties and integrity guarantees. Numerous systems that have come to be termed as "end-to-end verifiable" have been developed using a variety of techniques. These E2E-verifiable systems allow voters to check for themselves that their votes are properly counted and thereby achieve the same kinds of assurances they have when banking or shopping. However, until recently these systems failed to give adequate attention to the human element. If secret-ballot elections were conducted among entities with extensive intrinsic computing power, then current solutions would be ideal. But unaided humans cannot realistically be expected to encrypt data. This leaves two likely alternatives. If voters use their own trusted devices, then the devices could retain information that enables vote-selling and coercion; voters could even be casting their votes on devices given to them by coercers. Alternatively, if voters use devices provided by election officials or other parties, mechanisms must be provided to assure voters that these devices are acting according to their wishes.

More recent abstractions such as "software independence" and "evidence-based elections" have been developed to capture the integrity properties desired in elections. But systems have not been developed which achieve these properties together with all the other essential requirements of practical elections. For instance, many of the existing systems allow voters to determine whether or not their votes have been accurately counted, but few give voters who discover mishandling of their votes any evidence that can be used to demonstrate this error to third-parties. (The fundamental difficulty is to demonstrate that a vote has not been counted properly without revealing the contents of the vote.) Providing this kind of "dispute resolution" is a major challenge in the design of election systems.

Tremendous progress has been made in the past few decades. We can now build voter-friendly poll-site election systems that achieve full end-to-end verifiability and have properties far superior to what voters have come to expect. We have also made substantial progress towards the dream of secure, high-integrity online voting, but significant problems remain to be solved before we can responsibly suggest that voting from home is a viable option.

This book explores recent innovations in both poll-site and remote voting systems and their application throughout the world. The requirements of elections are analyzed, the available tools and technologies are described and a variety of modern systems are presented in detail together with discussions of deployments. This is an invaluable resource for election professionals, researchers and policy makers alike.

Josh Benaloh
Microsoft Research