Preface

The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate recordkeeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.

— Privacy Protection Study Commission, *Personal Privacy in an information Society*, July 1977

Paper-based communication and transaction mechanisms are being replaced by electronic mechanisms at a breath-taking pace. On the one hand, this transition improves security and efficiency, and opens up a mind-boggling range of new opportunities. On the other, it greatly increases the scope for identity fraud and erodes privacy in a manner unimaginable just a couple of decades ago. If the prevailing ideas about how to secure the global information highway are left unchallenged, then it will not take long before everyone is forced to communicate and transact in what will be the most pervasive electronic surveillance tool ever built.

What this book is about

This book proposes highly practical cryptographic building blocks that can be used to design privacy-protecting electronic communication and transaction systems. The new techniques allow individuals, groups, and organizations to communicate and transact securely, in such a way that at all times they can determine for themselves when, how, and to what extent information about them is revealed to others, and to what extent others can link or trace this information. At the same time, the new techniques minimize the risk of identity fraud, overcome many of the efficiency and security shortcomings of the currently available mechanisms, and offer a myriad of benefits to organizations. They can be implemented in low-cost smartcards without cryptographic coprocessors, admit elliptic curve implementations with short keys, and encompass today's views about digital certificates and public key infrastructures as a special case.

The new techniques are beneficial in any authentication-based communication or transaction environment in which there is no strict need to identify certificate holders at each and every occasion. The only acceptable role, if any, for identity certificates in such environments is to facilitate registration in case certificate applicants must be identified; this is similar to the way in which drivers' licenses and passports are traditionally used to acquire a permit or some other kind of authentication proof.

Any subset of the presented techniques (with the exception of those with conflicting objectives) can be applied in combination. This facilitates a cookbook approach towards designing electronic communication and transaction systems. Applications of special interest include, but are not limited to: electronic cash; digital pseudonyms for public forums and virtual communities (such as Internet news groups and chat rooms); access control (to Virtual Private Networks, subscription-based services, Web sites, databases, buildings, and so on); digital copyright protection (anonymous certificates permitting use of works); electronic voting; electronic patient files; electronic postage; automated data bartering (integration with standardization efforts such as P3P is easy); online auctions; financial securities trading; pay-per-view tickets; public transport ticketing; electronic food stamps; road-toll pricing; national ID cards (but with privacy); permission-based marketing; Web site personalization; multi-agent systems; collaborative filtering (i.e., making recommendations to one person based on the opinions of like-minded persons); medical prescriptions; gift certificates; loyalty schemes; and, electronic gambling. The design of specific applications is outside the scope of this book, though.

How the book is organized

Chapter 1 examines the role and the importance of digital certificates in communication and transaction mechanisms. It evaluates the major trends, and points out their security, efficiency, and privacy shortcomings. It also contains an outline of the techniques in the remainder of the book. While it is not necessary to read this chapter to understand the remainder of the book, much of the motivation would be missed.

Chapter 2 gives an overview of preliminary cryptographic notions and techniques, and introduces several new cryptographic primitives that are central to the constructions in the remaining chapters.

Chapter 3 presents certificate showing protocol techniques that enable the selective disclosure of personal (and other) data, and analyzes their privacy and security properties. This chapter should not be read without first reading at least parts of Chapter 2.

Chapter 4 presents certificate issuing protocol techniques that enable an issuer to encode attributes into certified key pairs that are unlinkable and untraceable in all other respects, and analyzes their security. This chapter builds on Chapter 2, but may be read independently of Chapter 3.

Chapter 5 describes how to combine the showing protocol techniques of Chapter 3 with the issuing protocol techniques of Chapter 4, and introduces a variety of additional techniques to improve privacy and security. For instance, software-only techniques are described for implementing limited-show certificates and for discouraging certificate holders from lending their certificates. This chapter builds on Chapters 2, 3, and 4.

Chapter 6 shows how to lift the techniques of the preceding three chapters to a setting in which certificate holders use smartcards or other tamper-resistant devices. Many security, efficiency, and functionality benefits are realized in this setting without adding complexity and without downgrading privacy. We also show how to tune our smartcard-enhanced protocols to accommodate any degree of privacy desired. The material in this chapter draws on all four preceding chapters.

The Epilogue argues that privacy is best protected by supplementing privacy-enhancing techniques (such as those developed in this book) with legislative measures. To support this claim it is shown how non-technical approaches toward privacy fail. The popular approach of "key escrow" is examined as well, and it is argued that this approach does nothing but mislead individuals into believing that they have privacy.

Acknowledgments

This book is an updated version of my self-published dissertation of September 1999. The unconventional history of how that dissertation came about can be found in the acknowledgments section of the dissertation, and is not repeated here.

My thanks go to my parents Jan and Bea, and to Vera and her parents Wil and Wim, for their support and encouragement throughout the years.

I am indebted to Professor Richard Gill, who in 1991 brought me in contact with the subject of cryptography and through his enthusiasm and encouragement got me hooked.

My gratitude also goes to Professors Ron Rivest, Claus Schnorr, and Adi Shamir, for taking place in my thesis reading committee and providing helpful suggestions and comments. Dr. Berry Schoenmakers of Eindhoven University of Technology also provided insightful comments on the draft dissertation.

Finally, I thank all those individuals and organizations around the world who are contributing in a positive manner to protect privacy. Your efforts, ranging from Internet discussions and press clippings to extensive resource archives and in-depth studies, have been an important source of inspiration to my work.

Stefan Brands
Montreal
April 30, 2000