SpringerBriefs in Computer Science

More information about this series at http://www.springer.com/series/10028

Hilarie Orman

Encrypted Email

The History and Technology of Message Privacy

Springer

Hilarie Orman
Purple Streak, Inc.
Woodland Hills, UT
USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-21343-9 ISBN 978-3-319-21344-6 (eBook)
DOI 10.1007/978-3-319-21344-6

Library of Congress Control Number: 2015944454

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

Like most people, I hope that my email is only being read by the people I send it to, but I realize that my hope is unfulfilled by ordinary email technology. Though almost everyone recognizes the importance of Web site security, their email, which might be much more personal, is rarely protected. In light of the unending revelations of insecure practices by Web site owners and the general uneasiness over surveillance by governments, a few people suggested to me that email privacy would be worthwhile. I was pleased to find that almost all my computing devices had preinstalled email clients with privacy controls.

Mind you, this was not surprising to me, because I first used secure email about twenty-five years ago. I felt that I understood the underlying cryptology and Internet protocols, if not in detail, at least in general design. How hard could it be to use today's tools? I set out on my secure email adventure with as little understanding of my task as a neophyte hiker with ill-fitting boots.

As I started on the journey, I made many informal queries among security-conscious, computer-savvy people about their use of encrypted email. Few of them had much experience with it, and it seemed that those with the most background had the most negative opinions. "Is it really that bad?" I wondered.

My first experiences were positive. Almost all the email systems that I had access to were supplied with software for encrypting and signing messages. It was a little bit difficult to find out where the controls were (hint: find the "Advanced" tab), and for some of them, I had to download additional software, but overall it went well. Then, I had to approach the problem of getting keys and configuring my email readers to use them. This presented some challenges, and I stumbled here and there, finally reaching a satisfactory state.

A stranger in a strange land, I found no one to share my adventure. Even though I correspond regularly with experts in computer security, no one I knew was interested in exchanging secure email. Checking over several years of past email, I could see little evidence that anyone I knew had the necessary prerequisite of the all-important public key: Fewer than one person in a thousand used the simple and unobtrusive signed email. I implored a few people to take the secure email plunge. Some initial experiments went awry, and I had to convince my correspondents to

keep trying to find the magic controls for accepting my keys, and I had to accept their keys. Strange error messages ensued. We forged on.

The experience was like treading over a rocky and distorted landscape without GPS. In each case, I reached my goal, but I began to understand how this technology that started out so bravely 25 years ago had shifted, fractured, and bent to become a frustrating terrain. I hope that those who read this book will understand the geology of the landscape and the well-trodden trails so that they can become skilled users of secure email and trail guides for their correspondents.

This is not a cookbook for using secure email nor a guide to buying a commercial email product. Such an effort would have to encompass too many email systems and key management utilities. What I have tried to accomplish is to show that underneath all the menus and tabs, there is machinery that carries out an understandable process of building secure messages and processing them on receipt. With this background, the various email systems make sense, and when things go wrong, the oddly terse error messages can lead to solutions for otherwise frustrating problems.

Beyond being not-a-cookbook, this is not primer on cryptography. There is material that explains some basic concepts, particularly how security depends on keys and why there are different kinds of keys. Understanding these concepts makes it easier to understand why there are so many choices to be made when one first embarks on the secure email adventure.

Many people helped me uncover the early history of email encryption. Marv Schaefer, Dennis Branstad, Ruth Nelson, Steve Kent, Ray Tomlinson, Dave Dyer, Doug Dodds, and Austin Henderson helped me uncover the all-but-forgotten history of BBN's encrypted email. Matt Bishop remembered the Unix public key message utility and its inner workings. Dave Balenson was generous in sharing his briefing materials and recollections of the IETF standards developed in the 1980s and 1990s. Jim Galvin's recollections about the IETF standards were equally generous and helpful. Mark Feldman provided archives of the PEM developers' email list from the 1990s.

Jon Callas was patient and helpful in answering my questions about the PGP specification and its interpretation. Tolga Acar had helpful observations about a popular email application. Don Cohen helped with my encrypted email experiments.

Richard Schroeppel was ever present to answer all my mathematical questions and made countless cups of coffee and scoured Utah County for good take-out food to sustain the two of us during the endeavor of writing this book.

Contents