Computer Insecurity

Dr. Steven Furnell is the head of the Network Research Group at the University of Plymouth in the United Kingdom and an Associate Professor with Edith Cowan University in Western Australia. He specialises in computer security and has been actively researching in the area for 12 years. During this time he has contributed to a number of UK and European projects, as well as presenting his work and findings at a variety of international events. Dr. Furnell is a Fellow and Branch Chair of the British Computer Society (BCS), a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), and a UK representative in International Federation for Information Processing (IFIP) working groups relating to Information Security Management, Network Security and Information Security Education. He is also a frequent reviewer for a variety of technology journals covering Internet and security issues, as well as the author of over 140 papers in refereed international journals and conference proceedings. Dr. Furnell's first book, *Cybercrime: Vandalizing the Information Society*, was published by Addison-Wesley in 2001.

Steven Furnell

Computer Insecurity

Risking the System

With 30 Figures

Springer

Steven Furnell, BSc (Hons), Phd, CEng, FBCS, CITP University of Plymouth, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2005923528

ISBN-10: 1-85233-943-8
ISBN-13: 978-1-85233-943-2
Springer Science+Business Media
springeronline.com

Typesetting: SPI Publisher Services, Pondicherry, India
Printed and bound in the United States of America
34-543210 Printed on acid-free paper SPIN 11317289

Preface

Security is one of the most significant issues facing the owners and users of computer systems in the Internet age. Although it has ostensibly been on the agenda for the last two decades, this does not mean that people fully understand the issue, or indeed how it might relate to them. Surveys still reveal a significant lack of awareness, as well as a lack of adherence to good practices. In addition, media reports frequently highlight the occurrence of incidents, even affecting high-profile organisations that we might instinctively assume are the most likely to be protected. These factors suggest that, although people acknowledge the issue, they may not truly appreciate the potential impacts or the role that they have to play. In parallel with this, the use of the Internet and the web has drawn more attention to the need for protection. Applications such as e-commerce and e-banking mean that security has become as much of an issue for individuals as it has been for businesses. As such, it is relevant for people at all levels to have an appropriate understanding of the surrounding issues and what is at stake. However, it is often apparent that this understanding is lacking, and while people may pay lip service to the importance of security, many fail to appreciate that they have assets requiring protection, and often stop short of making a real commitment. Similarly, some may have misunderstood or overlooked their risks, with the consequence that their attempts at protection are misdirected or inadequate. Meanwhile, others may simply assume that security is someone else's problem. The aim of this book is to show that security is an issue that affects us all.

There are, of course, many excellent security books already on the market, and so a legitimate question would be to ask why another one is necessary. The basic answer is that, while many existing titles focus quite heavily on *what* you need to secure and *how* you can do it, they do not devote much attention to *why* security is needed and what can happen without it. This is fine if potential readers have already accepted the importance, and understand how it relates to them, but if they do not see it as their problem, then they will be unlikely to benefit. This book consequently approaches security issues from a different standpoint. It discusses various ways in which systems and organisations may be vulnerable, the ways in which those vulnerabilities may be exploited, and the problems that can occur as a result. The intention is to give readers the necessary incentive to reassess their own practices, or indeed those of their organisation.

The chapters that follow are structured according to seven key themes, addressing a range of security issues, real-world examples, and related observations that demonstrate why we need to get protected. Although the book does not claim to

provide an exhaustive analysis of the potential problems, it does aim to boost awareness in critical areas by providing evidence to show the varied causes, manifestations, and victims of incidents—all of which adds up to an issue that cannot be ignored.

Chapter 1 sets the scene by presenting a general introduction to computer security and highlighting the basic principles that relate to both individuals and organisations. Evidence is presented to show that security is a constant problem, occurring within a society that depends heavily upon information technology. At the same time, however, having to deal with the problems is not always a welcome prospect, and so despite the need for protection, an atmosphere of insecurity is often able to flourish.

The main message of Chapter 2 is that if vulnerabilities are present, then things will go wrong eventually. In some cases, security is overlooked because people are unaware of the relevant information, whereas in other cases it would be more accurate to say that the issue is simply ignored. In either event, the significance is not properly perceived until it is too late, and the discussion provides a variety of examples to demonstrate why an informed approach is preferable to acting on blind faith.

Having considered scenarios in which security is lacking altogether, the message of Chapter 3 is that even the best security measures can be undermined if people do not understand them or do not take them seriously. Various examples are presented to highlight what can happen when the initial steps have been taken but are not followed through properly. A significant theme of the discussion concerns getting security into the minds of IT users, all of whom must play their part and be given a clear and consistent message about the importance of maintaining it.

Chapter 4 attempts to dispel the myth that security is someone else's problem, and the discussion demonstrates, by way of real-life examples, that problems can affect everyone—from large corporations, to small organisations, down to individuals. It also draws attention to the fact that there is no such thing as 100% security, and that no matter how much attention is devoted to it, the problem can never be considered solved once and for all.

If systems and data are not appropriately protected, then they are effectively open to attack. Chapter 5 illustrates this point by considering various threats that can result from deliberate and targeted activities, with examples ranging from external hackers and distribution of malicious software, to threats from within an organisation that are posed by its own staff. The discussion also highlights some surrounding problems, such as when a lack of security leads to our data being placed at unnecessary risk, as well as when others actively set out to steal it.

Chapter 6 highlights that even when we do our bit to protect ourselves, we are still very often dependent upon the attitudes and assistance of external parties. One issue here is the attention to security by software vendors and service providers. The discussion demonstrates that although we may assume security has been addressed, there are often vulnerabilities that we must still be aware of and act upon. Another dependency arises when seeking appropriate expertise to help us with security, and if we want the job done properly there is a clear need for professional competence.

As such, the chapter concludes by considering where we might look to find suitably qualified people.

The final chapter begins by summarising the main issues from earlier discussions; it then considers how organisations might be encouraged to take security issues more seriously. It also gives consideration to some of the contexts in which future threats and vulnerabilities are likely to occur, before concluding with some brief advice on what to do in order to start improving protection.

All of the chapters are presented (as far as possible) in layman's terms, so that readers without a detailed technology background can appreciate the many forms that problems may take, and the consequences that can result. The examples are presented from a variety of perspectives, with topics of relevance to both organisations and individuals. As such, it is hoped that the material will be of interest to a broad audience, including business professionals, students and other members of the general public who want to know why security is an issue that affects them. Additionally, although the main arguments will not be new to them, security professionals will be able to use the material help justify security to others, as well as to remind themselves of why they are needed in the first place.

Acknowledgements

This is my second book, and in many ways it has been more difficult to write than the first time around. Whereas the previous book was specifically focused around issues relating to computer crime and abuse, this one began with a much broader canvas—and consequently offered a much greater range of discussion topics to choose from. I hope that the themes I have ultimately chosen to look at will prove as interesting to read about as they were to research.

Although there is only one name on the front cover, a number of people have actually been involved in the development of this book. I would firstly like to thank Helen Callaghan at Springer, for her considerable advice and assistance, and for helping me to get the material published. Sincere thanks are also due to Nathan Clarke, Vassilis Dimopoulos, Paul Dowland, Michael Evans, Bogdan Ghita, Maria Papadaki, and Prof. Peter Sanders, who all gave up their time to help me by reading and commenting on the early drafts. Their thoughts were extremely valuable in enabling me to decide which bits of the text should stay, and which could go, and I am very grateful to all of them.

Above all, this book is dedicated to my late father, Maurice Furnell, who did not get a chance to read it.

Contents