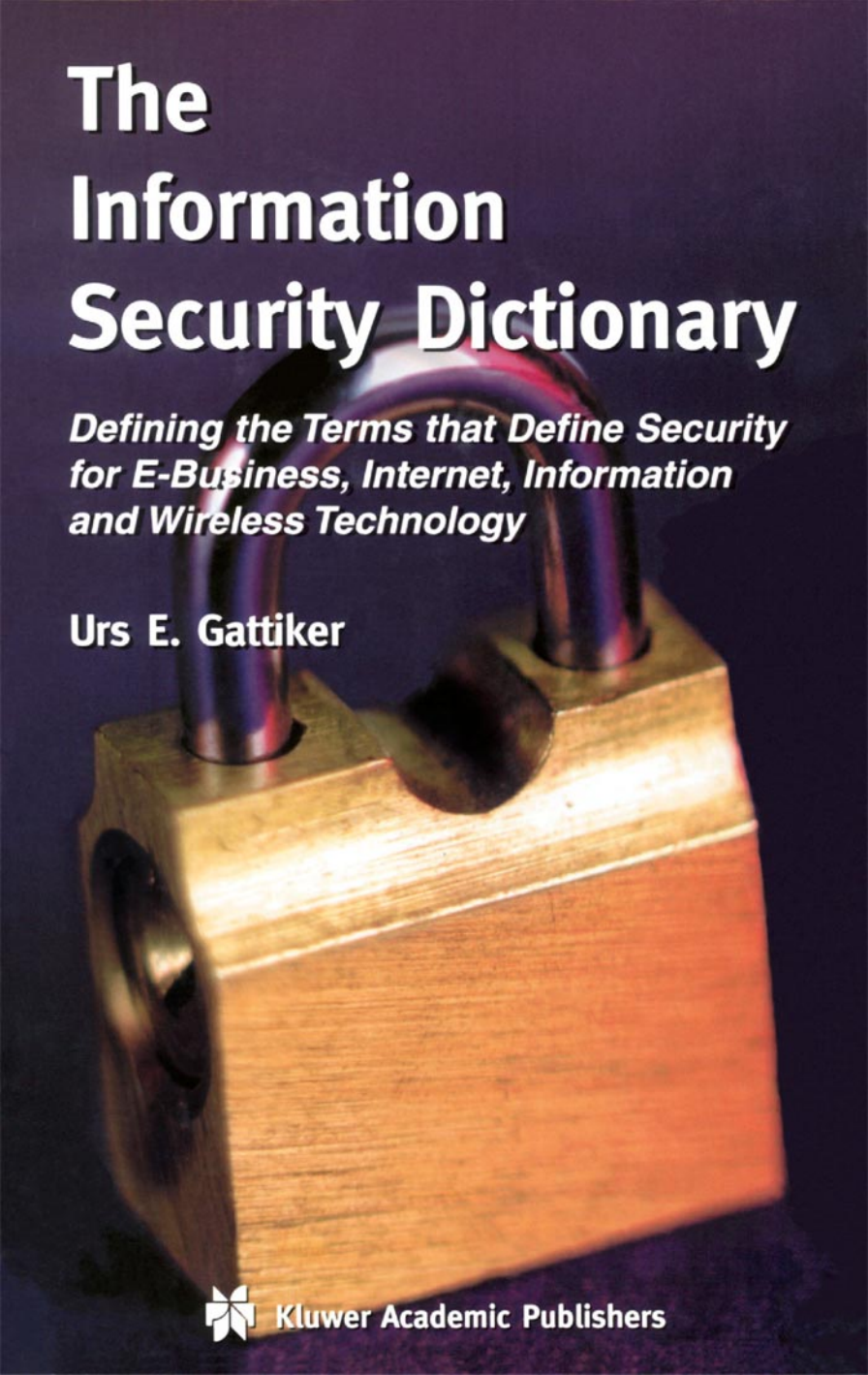
The Information Security Dictionary

Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology

Urs E. Gattiker



Kluwer Academic Publishers

THE INFORMATION SECURITY DICTIONARY

Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology

THE KLUWER INTERNATIONAL SERIES IN ENGINEERING AND COMPUTER SCIENCE

THE INFORMATION SECURITY DICTIONARY

Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology

by

Urs E. Gattiker
Information Security this Week – Denmark
CASEScontact.org
EICAR.org
and
International School of New Media (ISNM)
University of Lübeck, Germany

KLUWER ACADEMIC PUBLISHERS
NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 1-4020-7927-3
Print ISBN: 1-4020-7889-7

Created in the United States of America

Visit Springer's eBookstore at: http://www.ebooks.kluweronline.com
and the Springer Global Website Online at: http://www.springeronline.com

This book is **dedicated to the memory of:**

George Lermer

The dean who hired me for my first tenure-track job at the
University of Lethbridge, Alberta, Canada,
who became my mentor and dear friend.
He died March 15, 2003 while skiing at
Castle Mountain (Canadian Rockies).

This page intentionally left blank

Contents

If you would like to see a new word added to the **IT Security Dictionary**, please write to:

Dictionary@WebUrb.com

List of Figures

This page intentionally left blank

List of Tables

This page intentionally left blank

Preface

Something for Everyone

If this book is to succeed and help readers, its cardinal virtue must be to provide a simple reference text. It should be an essential addition to an information security library. As such it should also serve the purpose of being a quick refresher for terms the reader has not seen since the days when one attended a computing science program, information security course or workshop.

As a reference work, **THE INFORMATION SECURITY DICTIONARY** provides a relatively complete and easy-to-read explanation of common security, malware, vulnerability and infrastructure protection terms, without causing much damage to the usually slim student pocketbook.

This dictionary can help non-specialist readers better understand the information security issues encountered in their work or studying for their certification examination or whilst doing a practical assignment as part of a workshop.

This book is also essential to a reference collection for an organization's system personnel. Special attention is paid to terms which most often prevent educated readers from understanding journal articles and books in cryptology, computing science, and information systems, in addition to applied fields that build on those disciplines, such as system design, security auditing, vulnerability testing, and role-based access management. The dictionary provides definitions that enable readers to get through a difficult article or passage. We do not, for the most part, directly explain how to conduct research or how to implement the terms briefly described.

The emphasis throughout, is on concepts, rather than implementations. Because the concepts are often complicated, readers may find that a definition makes sense only after it has been illustrated by an example. Thus explanations and illustrations are sometimes longer than the definitions.

Quite a few terms are included that might not meet strict definitions of "information security"—for instance, validity, reliability, attitudes, cognition, and

digital divide. But they, and several others like them, are defined because they meet the main criteria for inclusion:

The words pop up fairly often, in more than one discipline, and many people are unsure of the meaning.

When learning any language, beginners will sometimes be frustrated because they have to look up words in the definition of the term they just looked up. By writing the definitions in ordinary English whenever possible, we have tried to keep this unavoidable annoyance to a minimum. However, there is simply no escape when defining advanced concepts that are built upon several additional basic concepts. Those terms, also defined in this dictionary:

- start with a capital letter (e.g., Computer Literacy), or may be simply
- listed in the text or, finally, be
- added to a term or definition in brackets in the paragraph or at the end (see also Computer Literacy).

Hence, the reader is able to find the other term quickly in order to understand the larger picture.

As in any language, in Information Security, more than one word may be used to express the same idea. In such cases, we have defined fully what we believe to be the more common term. Others are briefly defined and cross-referenced (Computer Literacy). Nonetheless, we have not tried to stipulate the "proper" labels for concepts that appear under more than one name. Neither have we specified the "correct" use of terms that are used in different ways. In short, we have attempted to be:

inclusive and descriptive

not exclusive and prescriptive. The goal throughout has been to provide a comprehensive dictionary of terms that will increase access to works in the engineering, medical, social and behavioral sciences.

While not every company will use the same security tools and services, a company must use a level of security that is appropriate for safeguarding its functions. There is no such thing as 100 percent security, but striving to reduce the potential risk for a threat to materialize makes business sense.

Similarly, there is no free lunch. Satisfactory security for critical IT infrastructures can hardly be attained without the necessary human, technical and financial resources.

Finally, an important step toward greater security against threats from within and without, is achieved by talking the same language—improving communication and ultimately improving results.

This dictionary is a step toward developing similar meanings and a more unified interpretation of different terminology, categories and events—a crucial step toward a discipline's maturation.

There are rarely straightforward solutions to real world issues—especially in the field of security. This dictionary is an essential tool to help solve those real world problems by providing the foundation we need to communicate effectively amongst each other—our work vocabulary.

By covering situations that apply to everyone from the seasoned Systems Administrator or student of Computer Forensics, to the security curious home user, the Dictionary distinguishes itself as an indispensable reference for security-oriented individuals.

Many events result in loss of data or damages of IT hardware and software. Theft of equipment is part of physical object management. Furthermore, environmental threats (e.g., earthquakes, floods and power surges) and software bugs are also of concern.

This glossary focuses on information, e-business, computer and wireless security as encompassing, but not necessarily limited to:

1) the protection of computer files containing digitally stored information:
   a) ensuring the accessibility of computer and network systems and, as well,
   b) protecting the integrity and confidentiality of data;
2) protecting access processes to certain operations, thereby reducing the risk for role-based access being violated or compromised.

Statistical definitions are included since IT security is moving rapidly toward a more established scientific discipline, which supplies research used for guidelines applied in corporate settings.

This page intentionally left blank

Acknowledgements

Many people have aided my development as a researcher and student of technology and, in particular, the Internet and security. This book provides a welcome occasion for me to express my indebtedness and appreciation.

This book would have never been taken on as a task and most likely remained unfinished if I would not have passed through a stage, whereby I was trying to figure out a few things concerning my private life and professional career. Whilst reflecting and not being particularly productive, Inger Marie Giversen urged me in no uncertain terms to write these things down. She felt that I needed to clarify some of these issues and further develop the vocabulary for my own benefit. Subsequent use might even help others working in information security and striving in protecting their organization's or country's critical infrastructures. She has an uncanny ability to see and formalize things in a clear and concise fashion, also where a field of inquiry or discipline might move toward. She is a true **trail blazer** and in this case I definitely benefited from her visionary understanding of IT security in the context of September 11, bio-terrorism and the spread of medical viruses. Hence, she deserves a big thank you, yet any mistakes are mine.

Stefano Perlusz, my former Ph.D. student and dear friend, once told me while we were standing in his kitchen getting supper together that I needed to carefully focus my work and interests. Over a salmon steak, beer and a delicious salad, he urged me to either focus more on IT security and risks in information technology, or else just simply drop the ball and vanish into the sunset. I have taken his advice to heart, and worked diligently to focus more on the area of information security (http://Security.WebUrb.dk, http://www.CASESkontakt.de, http://www.CyTRAP.org for examples). Any omissions remain the sole responsibility of the author:-).

Rainer Fahs remains another fixture in my private and professional life. We are so different in more ways than one, or Ying and Yang. His experience in