

# 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

©2004 Springer Science + Business Media, Inc.

Print ©2004 Kluwer Academic Publishers  
Boston

All rights reserved

No part of this eBook may be reproduced or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without written consent from the Publisher

Created in the United States of America

Visit Springer's eBookstore at:  
and the Springer Global Website Online at:

<http://www.ebooks.kluweronline.com>  
<http://www.springeronline.com>

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

# **George Lerner**

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

<b>List of Figures</b> .....	ix		
<b>List of Tables</b> .....	xi		
<b>Preface</b> .....	xv		
<b>Acknowledgements</b> .....	xix		
<b>Why is IT Security Important</b> .....	xxiii		
<b>About This Dictionary</b> .....	xxvii		
<b>About The Author</b> .....	xxix		
<b>How to Use This Dictionary</b> .....	xxxi		
<b>A</b> 1-31	<b>B</b> 32-44	<b>C</b> 45-76	<b>D</b> 77-105
<b>E</b> 106-127	<b>F</b> 128-136	<b>G</b> 137-138	<b>H</b> 139-149
<b>I</b> 150-182	<b>J</b> 183-189	<b>K</b> 190-192	<b>L</b> 193-198
<b>M</b> 199-218	<b>N</b> 219-222	<b>O</b> 223-226	<b>P</b> 227-260
<b>Q</b> 261-262	<b>R</b> 263-281	<b>S</b> 282-318	<b>T</b> 319-339
<b>U</b> 340-345	<b>V</b> 346-359	<b>W</b> 360-373	<b>X</b> 374
<b>Z</b> 375			
<b>Epilogue: Critical Infrastructure Protection (CIP)</b> .....	376		
<b>Appendices</b> .....	381		
<b>Suggestions for Additional Resources</b> .....	383		
Appendix 1 On-Line Databases for Vulnerabilities and Security ...	384		
Appendix 2 Dictionaries & Encyclopedias .....	386		
Appendix 3 Miscellaneous Resources .....	388		

Appendix 4 Legislation and Regulation – European Union . . . . . 392

Appendix 5 Legislation and Regulation . . . . . 396

Appendix 6 Standards and Best Practice . . . . . 398

Section A . . . . . 398

Section B . . . . . 400

Security and Utility Tools . . . . . 403

Appendix 7 ‘Nearly’ or Outright Free Security Tools for System  
Administrators . . . . . 403

Appendix 8 ‘Nearly’ or Outright Free Security Tools for  
Home Users . . . . . 405

Awareness Raising – Skill Development . . . . . 407

Appendix 9 Newsletters . . . . . 407

Appendix 10 Alerts and Advisories . . . . . 410

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

## List of Figures

<b>Figures</b>	<b>Description</b>	<b>Page</b>
Figure 1	Basic model about vulnerabilities resulting in unauthorized access or use of processes.	4
Figure 2	Prevention mechanisms for reducing the risk of unauthorized access while protecting against physical, syntactic and/or semantic attacks.	24
Figure 3	Attack resulting in unauthorized access and use of processes with various results as outcome thereof – prevention mechanisms to increase security.	25
Figure 4	A taxonomy for risk management.	166
Figure 5	Taxonomy of malicious code or malware.	201

*This page intentionally left blank*

## List of Tables

<b>Table</b>	<b>Description</b>	<b>Page</b>
Table 1	Value of information – asset approach	16
Table 2A	Value of information – hard costs	17
Table 2B	Value of information – soft costs	19
Table 2C	Asset value of data/information or object	20
Table 2D	Assurance: Security – costs and benefits	21
Table 3A	Taxonomy of attacks	23
Table 3B	Attributes of attacks	26
Table 3C	Elements of attacks	27
Table 4A	Biometrics and authentication – access controls	36
Table 4B	Authentication – access controls	37
Table 4C	Biometrics and authentication – less effective access controls	38
Table 5A	Critical Information Infrastructure Protection (CIIP) – information sharing approaches	49
Table 5B	Critical Information Infrastructure Protection (CIIP) – trusted information sharing network	50
Table 5C	Confidentiality, Integrity, Availability of Data, User Accountability, Authentication and Audit (CIA-UAA)	60
Table 6	A baseline for security – taxonomy of policies for enhancing and supporting critical infrastructure protection (CIP) efforts	62
Table 7A	Damages – using the asset and policy document approach to quantify losses	80
Table 7B	Defense – what it might entail	87
Table 7C	Defense – possible escalations	89

Table 8	Distributed denial-of-service (DDoS) attack – tools to reduce the risk for a successful DDoS	102
Table 9	E-government	108
Table 10A	Criteria for an electronic (e-voting) system – voter and votes	110
Table 10B	Criteria for an electronic (e-voting) system – election system and process	112
Table 11A	Encryption-decryption algorithms	119
Table 11B	Encryption-decryption algorithms	120
Table 12	Firewalls	132
Table 13A	System safety and security - system complexity	161
Table 13B	System safety and security – failure of safety	162
Table 13C	System safety and security – human behavior and techno babble	163
Table 14A	Information theory	168
Table 14B	Information as a concept	170
Table 15A	Intrusion detection	176
Table 15B	Intrusion Detection System (IDS) – evolving terminology	177
Table 15C	Intrusion Detection System (IDS) – calculating Return on Investment (ROI)	180
Table 16A	Jurisdiction	184
Table 16B	Justice, ethics, morality and rights – Or how do these concepts relate to code of conduct	187
Table 17A	Key management	191
Table 17B	Key recovery (KR) – trusted third party encryption (TTPE)	192
Table 17C	Learning and type of training	194
Table 17D	Information security skills (ISS)	196
Table 18A	Defining malware – a simplified structure	202
Table 18B	Vulnerabilities and malware	203
Table 18C	Types of malware – categorization	204
Table 19A	Digital divide and broadband connection	207
Table 19B	Reducing digital divide – different technologies with different suppliers	209
Table 20A	Password issues	231
Table 20B	Password use, policy and best practice	233
Table 20C	Vulnerabilities and malware - managing patches and upgrades – corporate users	237
Table 20D	Vulnerabilities and malware - managing patches and upgrades as a Small and Medium-Sized Enterprises (SMEs) or a home user	239

**List of Tables****xiii**

Table 21A	Policies and IT-resources – appropriate user behaviors	247
Table 21B	Privacy and asymmetric information spaces – definition and principles	253
Table 21C	Privacy and asymmetric information spaces – properties and boundaries	254
Table 22A	Cognitive and emotional components of risk – perception and worry	273
Table 22B	Risk – experts versus lay-people	274
Table 22C	The business perspective of internet and IT security risks	275
Table 22D	The user’s perspective of internet and IT security risks	275
Table 22E	Network security risks – visibility and vulnerability	277
Table 23A	Schemata with the scientific roots of information security – the birth of securematics	287
Table 23B	Defining security and safety for information systems-related products and services	292
Table 23C	Security engineering versus safety engineering	294
Table 23D	Security engineering for a small and medium-sized enterprise (SME)	304
Table 24A	Differentiating threat, vulnerability and risk at one glance	325
Table 24B	Typology of threats: Two main types	326
Table 24C	Taxonomy for structured and unstructured threats	327
Table 24D	Further classification of typology of threats and their taxonomy	328
Table 24E	Definition of criteria to be used for evaluating threat level for malware and vulnerabilities	330
Table 24F	Threat level definition – malware	331
Table 24G	Threat level definition – software/operating system vulnerabilities	332
Table 25	Types of viruses – categorization	353
Table 26	Taxonomy of vulnerabilities	358
Table 27A	Constituencies for a WARP	361
Table 27B	Focus and functions for a WARP	361
Table 28	Leaks and security lapses in Wi-Fi 802.11	370
Table 29	Worms	372

*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