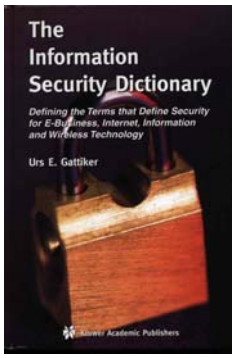
BOOK REVIEW

DICTIONARY DEFINITIONS

Eddy Willems
NOXS and EICAR, Belgium

Title: The Information Security Dictionary
Author: Urs E. Gattiker
ISBN: 1-4020-7889-7
Publisher: Kluwer Academic Publishers



Earlier this year I found myself searching for a book which would help my co-researchers (see *VB*, August 2004, p.10) to define some of the terms they would come across within the field of information security. It was at that moment that *The Information Security Dictionary* appeared.

The Information Security Dictionary attempts to explain the terms that define security for e-business, Internet, information and wireless technology. It is written by Dr Urs E. Gattiker, who has co-authored other security-related books, such as *Viruses Revealed* (in 2001 with David Harley and Robert Slade).

The book has what I would call 'something for everyone'. The first edition defines over 1,200 of the most commonly used words in the security field, with particular attention being paid to the terms used most often in computer forensics, and those relating to malware, viruses and vulnerabilities.

This dictionary will help non-specialist readers understand the information security issues they encounter in their work or in studying for certification examinations – but it will also help the real IT security expert in pinning down a definition for a specific term or word.

The goal throughout has been to provide a comprehensive dictionary of terms that will increase access to works in all sciences. Even statistical definitions are included, since IT security is moving rapidly towards becoming a more established scientific discipline.

Special attention has been paid to terms which may prevent educated readers from gaining a full understanding of journal articles and books in cryptology and security and information systems, as well as applied fields that build on these disciplines.

A number of definitions have been included for terms that might not strictly be associated with information security – for instance: validity, reliability, attitudes and cognition. The author reasons: '[These words] meet the main criteria for inclusion: the words pop up fairly often, and many people are unsure of the meaning.'

The emphasis throughout the book 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 – as a consequence, the explanations and illustrations are sometimes longer than the definitions themselves.

As in any language, more than one word may be used to express the same idea. In such cases the author has included a full definition for what he believes to be the more commonly-used term, while the other terms are defined briefly and cross-referenced.

The rules used for the dictionary's listings are minimal but important to understand. For instance, when a term such as 'Virus' has several related terms (e.g. polymorphic virus), the related definitions may all appear as sub-entries under the definition of the main term ('virus'). Under the entry 'polymorphic virus' the reader is simply referred to the 'virus' entry for further explanation. This helps non-specialist readers to find their way around faster when dealing with unfamiliar terms.

The following is an example of a definition from the dictionary:

> '**Virus** is a segment of a computer code or a program that will copy its code into one or more larger 'host' programs when it is activated. Unfortunately, it also may perform other unauthorized actions at that time (see also Merging of attack Technologies, Trojans, Virology).
>
> 'To illustrate, Virus is a program that searches out other programs and infects them by embedding itself in them, so that they become Trojans. When these programs are executed, the embedded virus is executed as well, thereby propagating the "infection". This process tends to be invisible to the user.'

The book is well and logically structured, with clear figures and tables. The appendices provide one of the most comprehensive listings I have seen of informational dictionaries and other resources, with a good selection of URLs for some interesting and useful websites.

I was not always fond of the illustrations and definitions I found in this book. Certainly some experts will feel that a number of the definitions are not complete or that the illustrations are not always sufficiently strict. The dictionary could be considered a little too general for the more experienced security or anti-virus experts. Nevertheless, in my opinion the author has done a good job, and this dictionary is a must-have for anybody who works with or who is interested in information security.

This is yet another book to add to my ever-expanding anti-virus and IT security library. When will it end?