Review of the book

"Open Source Systems Security Certification"

by Ernesto Damiani, Claudio Agostino Ardagna, and Nabil El Ioini
Springer Science+Business Media, LLC, 2009

ISBN 978-0-387-77323-0

Meiko Jensen
Chair for Network and Data Security
Horst Görtz Institute for IT-Security
Ruhr-University Bochum, Germany

1 What the book is about

The major topic of this book is the rationale behind applying software security certifications (e.g. Common Criteria) to open source systems. At first glance, this seems to be a contradiction, because a security certification is usually given to a specific release of a specific software configuration, sometimes even only if running on a specific hardware or for a specific purpose, whereas open source systems like the Linux kernel undergo a constant development process that involves lots of code changes and usage shifts every day. Nevertheless, in order to use common open source products (like the Linux OS) in high-security areas like healthcare or e-government an appropriate security certification must be obtained.

The book starts with a broad overview on the core concepts behind every security certification. After introducing the basic notions and paradigms of access control techniques, some in-depth descriptions on test-based security certification and model-checking-based security verification are given. Both fields are involved in typical security certification mechanisms, since they provide detailed information regarding the measurable degree of security a software product gives. Test-based security certification, for instance, can be used to obtain detailed information on whether a given software product can stand the state-of-the-art set of known attacks, and also whether its functionality matches the assumptions thereon. Model checking, on the other hand, provides a provable level of correctness, hence safety, of the software system's behaviour.

Nevertheless, both approaches have their deficiencies when being used in a software security certification process. Test-based certification massively depends on the selection and processing of the particular test cases, whereas model checking tends to run into complexity issues known as the *state explosion problem.*

Based on these basic certification building blocks, the book continues with a detailed discussion of common security certification processes in the open source world, majorly based on some case studies that have been performed within the last years. The first case study discusses the application of a security certification according to the *Common Criteria (CC)* certification for a specific version of the Linux kernel (SLES8), giving very detailed information on how the Target of Evaluation was described and tested within the certification process, what benefits this process perceived from the *Linux Test Project (LTP)*, and whether and how this certification may be reused (in parts) for other Linux kernel certifications.

The second case study presents the ICSA approach of software security certification, which—in contrast to the Common Criteria—is based solely on running a set of applicable security-related tests specific for the type of software in certification. Using the example of the Endian firewall system, the book describes the certification process of ICSA, what assertions such a certification gives, and how the Endian firewall system performed in the ICSA certification evaluation.

In its conclusion, the book gives an excourse on the use of virtualization for setting up appropriate testing environments for test-based security certification processes, and the concludes with an outlook on what research challenges are to be tackled in order to reach long-term certification with maximum reusability.

2 What is the book like

The book provides its contents in the typical style of a set of research papers. Every chapter is dedicated to a single topic, giving a brief introduction and conclusion, as well as literature references for further reading. Though most of the chapters provide their information in a well-written, easy-to-understand manner, the reader is likely to loose focus due to the strong segmentation introduced by this approach. For instance, though every topic is linked to the overall approach of applying security certifications to open source systems, it is difficult to grasp the connections between all these topics, especially since the book does not provide a general ”solution” to the open source systems security certification problem. Merely, it provides every kind of knowledge required as a starting point for developing such a solution, but every time it comes to the application of the described topics to open source systems, the book refers to the outlook chapter (which then just lists the problems), or omits that information completely.

Furthermore, especially the case studies are presented with lots of technical details, such as listings of security objectives and threats to the *Common Criteria's Target of Evaluation*, here meaning the Linux kernel configuration in consideration. Though this is suitable for giving the reader an impression of how such lists look like in a CC security certification document, it rapidly gets annoying to read through lots of dry keyword lists with short descriptions of what they intend to mean.

To resume, the style of the book is rather a set of independent research book chapters than a continuously written essay.

3 Would you recommend this book?

The book actually gives a very nice introduction on each of the topics, so I recommend the book for everybody who wants to get a broad overview about the methods and techniques used in security certification. Being written as a research handbook, I would not directly recommend it to non-researchers. In the same line, one should not expect to get a step-by-step guide for obtaining a security certification, nor should one expect to find a real solution to the stated problem of open source systems security certification. However, the book provides valuable knowledge that I have not seen in this constellation before. Thus, I can recommend the book without restrictions to everybody who is intersted in extending one's perspective on how IT security is going to be treated in near-future real-world IT systems.

The reviewer is a Ph.D. student at the Horst Görtz Institute for IT Security in Bochum, Germany.