Review of the book

"Introduction to Network Security"
by Douglas Jacobson
Taylor & Francis, 2009

ISBN-13: 978-1-58488-543-6

Olivier Blazy, ENS/CNRS/INRIA, France

2010-01-18

1 What the book is about

As explained by the author, Douglas Jacobson, the books aims to explain network security. Instead of considering networks as a media of communication, he focuses on them as a source of security and insecurity. This book tries to highlight the main issues with networks where security was not part of the design process.

This book is divided into four main parts.

- The first part, entitled *Introduction to Network Concepts and Threats.* In this section, through 4 chapters, the author will give an overview of network architecture, explaining how layer works, how protocols are designed, with a full chapter about the Internet. And then he explains the taxonomy of attacks based on network (dividing it into 4 categories), there are those altering the protocol headers, those altering the packets using them for things they are not supposed to, those targeting authentication corrupting the identity of either the sender or the recipient, and those based on the volume of traffic (like DoS).
- In the second part, entitled *Lower Layer Security*, the author gives an overview, through 3 chapters, of Physical Network Layers protocols (Wired or Wireless), Non-physical Network Layer Protocols (like IPv4, IPv6, DHCP) with 6 different progressive scenarios to show how IP protocols are used, and then Transport Layer Protocols (TCP, UDP and DNS) with vulnerabilities and common countermeasures. It helps to understand which vulnerabilities may be present in a network layer and which mechanisms may be used to overcome those weak points (and explained that there are not many countermeasures for the transport layer).
- In the third part, entitled *Application Layer Security*, the author gives an overview, through 4 chapters, of application layers, e-mails (SMTP, POP, IMAP, MIME), Web Security (HTTP, HTML) and Remote Access Security (Telnet, rlogin, X-Windows, FTP, P2P). Each time, he shows some of the potential vulnerabilities and common countermeasures used to prevent them. Most of the time, network is considered on the Internet as a simple pipe, transmitting data without errors, this part helps to understand why this is false, and which tricks are used here again to patch these vulnerabilities.
- In the fourth and final part, entitled *Network-based Mitigation*, the author gives an overview, in a rather brief chapter, of common security devices (like firewalls, network-based intrusion detection (IDS), or network-based data loss prevention (DLP)). This chapter relates these solutions to the initial taxonomy, making a good conclusion to the journey done throughout the book.

The four parts are organized around a *define-attack-defend methodology*, which keeps the reader interested during the presentation of each concept, protocol and helps him understanding why some things are dangerous and why they were patched in a specific way.

2 What the book is like

In the book the author tries not to fall into the common trap of explaining security on higher levels and skipping the lower ones which may often be the most dangerous mistake. Therefore in the 4 parts, he will focus on networks, how they work precisely, which weakness are inherent and how to counter them. The book is divided into 4 parts with several chapters around the same topic. At the end of each chapter, the reader can find a small but really useful glossary, some references and some problems / experiments. In each chapter, you can find a lot of figures, often self-explanatory, which underline the different aspects explained throughout the chapter. You can also find excerpts from RFC which shows how things are designed.

The whole book tries to be self sufficient, the first part introduced a taxonomy of network-based attacks shows the readers what is at stake when you study Network Security, the next two are more didactic, and through some attacks explains how to increase the networks security, the final comes back to the taxonomy and highlights how the different vulnerabilities have been dealt with.

At the end of the book, there are some appendices. The first one is here to explain some basic cryptology notions like hash functions, symmetric key encryption, asymmetric encryption, signature, the second give details on how to deploy a lab environment required for the experiments to run at the end of each chapter and/or that can be employed as a test bed. The last appendix gives solutions to some of the homework proposed throughout the book. An index is present at the end of the book, and which let the reader uses it as a reference manual if needed.

3 Recommendation

It's not so easy to determine who is the best target for a given book. I guess this book can work for two different audiences: on the one hand students in Computer Science / Network Security might be interested, on the other hand security professionals can use it as a convenient reference book.

Students can easily understand how things work thanks to the different figures / definitions and if they need some precision they can read the corresponding section with the support of the previous figure. There is, indeed, a lot of figures but not too many. It's often hard to find the right balance but while reading the book I was nicely surprised to notice that I was able to find a graphic example when I need it, but that I never had to skip 10 pages to avoid a boring example. The global organization of the book is quite logical, and so students can see the different steps taken to build a secure environment and avoid most of the usual mistakes.

On the contrary, professionals will probably focus on specific subsections, while maybe using the figures only to summarize some of the notions. (Or to explain a notion to a neophyte). The different applied examples can give direct solutions to some problems. And again, as the security is studied from the lower layer, they can determine precisely on which ones they can work, and how to do it. (And how it will impact the overall security). As said before, the final index is really useful to transform the book as a quick reference manual, and if more information is needed, the bibliography at the end of each chapter will be useful.

A website (http://www.dougj.net/textbook) is provided to support the book, where the reader can find additional content, like instructor materials, slides to support the book, on-line tutorials, help to start the programming parts. It is not mandatory at all to understand the book, but it is a really nice addition.

From the reviewers point of view, the book is really well written, and easily understandable without lacking the rigor required in the domain. If I have to find some drawbacks I'd say that some parts are rather small and may be developed a little further. (However it's not ruining the global understanding) Another thing, the last part is rather too short too, and maybe other examples would have been appreciated. This book won't get dusty on my shelf, as it contains so many precious information, and is enjoyable. I'm really glad to have review it, as it helped me clarified some questions I had on Network Security.

The reviewer is a Ph.D. student at the Ecole Normale Supérieure, Paris, France.