Review of the book

"Guide to Computer Network Security"

by Joseph Migga Kizza
Springer, 2009

ISBN: 978-1-84800-916-5

Kilian David, M.Sc.
Dipl. Wirt.-Inf.

1 What the book is about

The book "Guide to Computer Network Security" is part of the Springer series Computer Communications and Networks. It is classified as a students research and self-study workbook which could also be used as a lecture for undergraduates. Therefore the author provides a particular homepage containing the different challenges (lasting one week, semester-long projects and topics for a master thesis or Ph.D.). In addition to this a syllabus is available summarizing the different chapters of the book into a (maximum) 15-week course. The chapters are seperated in three big parts, namely "Understanding Computer Network Security", "Security Challenges to Computer Networks" and the last and most extensive one "Dealing with Network Security Challenges". In the following a short summary of each chapter focusing on the main and most interesting points will be given.

2 Summary

After introducing the very basic methodologies of network topologies (like ISO/OSI, TCP/IP, physical devices and LAN technologies) the understanding of computer network security is described. In this chapter the so called CIA-concept (confidentiality – integrity – authentication) as requirement for a successful protection as well as non-repudiation and different security standards are presented. All information is given in a short an compact way which is easy to understand, even for readers who have never been active in this area of computer sciences. The following simple and advanced exercises give the reader a good possibility to review the topics and lessons learned. Since this described way of content-representation is used throughout the book, it is possible to get a very quick walk through during (possibly) three weeks. All you have to do is the following: There are 21 chapters. So if you want to get all of the content in a relaxed way, you only have to read one chapter a day (about 20 pages) and think about the simple and advanced exercises. Since they are not very challenging and only sometimes in the later chapters a little bit time consuming because of necessary research, you really can get it during the period mentioned above! OK, back to the content...

There is only one point in this second chapter I have to complain about. Since it is a book published at the end of 2009, I would expect that the presented information is state-of-the-art. Unfortunately, some of the standards presented are already outdated (ISO 17799) or have never been released in a final or work-in-progress version (CASPR). In my opinion the content concerning these frameworks and best-practices has to be reviewed and updated to ensure that current development and frameworks like ISO/IEC 2700$\{1, 2, 5, 6\}$, ITIL, SAS-70 are considered. Also missing is a disquisition on compliance or IT-compliance in conjunction with the requirements derived from the Sarbanes-Oxley Act (SOX) or other legislative regulations.

2.1 Part II: Security Challenges to Computer Networks

Chapter 3, "Security Threads to Computer Networks" first gives an historic overview about the sources of security threads. The motivation of the hacker community and the most devastating viruses are explained. Although this chapter *wants* to give an historic overview, it also looks – like mentioned above – a little bit outdated. The overview about the viruses end in 2003, an incident study conducted by Ernst & Young from 1997 (!) is referred to, a Computer Crime Survey from 2001 cited an so on. Since the book was published at the end of 2009, I was looking forward to seeing the current information from this rapidly growing area of research. But it seems that this chapter was already finalized in 2003.

Chapter 4 "Computer Network Vulnerabilities" describes four kinds of sources for vulnerabilities, which could result from design flaws, poor security management, incorrect implementation and Internet technology vulnerabilities. Here the problem in this chapter becomes obvious as no connection between the headline and the contents can be drawn. Additional content covers social engineering and only three minimized points about vulnerabilities assessment services. Chapter 5, "Cyber Crimes and Hackers" gives an elementary understanding about these topics. Unfortunately, the author is mixing up technical details (like different kind of DDoS-attacks), historical overviews (hacker, crackers, hacktivists) which confuses the reader to really point out the main approach of this chapter. Here, much more could have been expected from the currently available structures/threads of the so called "cyber crime economy".[1] Chapter 6, "Focusing on Hostile Scripts" mainly describes CGI-methodologies like handshakes and some of the possible security client-server problems. In addition to this some scripting languages are presented.

I think that this book is a good hands-on guide for practitioners because of giving a widespread overview about different topics. Every one of them is tried to capture so that you get an idea about what you should think about (deeply) if you really want to use it.[2] *Although the chapters are lacking of completeness and up-to-dateness they are nevertheless suitable for undergraduates and readers who have never heard about the topics. From a scientific book more detailed information about additional references and cross-checked or updated citations would have been expected. If you have the purpose to implement network security, this book is not suitable enough. Here, other books like the easy one from* Bless et al.[3] *or the complex and definite book from* Wang[4]*, which really covers the theoretical* ***and*** *practical aspects of understanding and implementing network security are recommended.*

Chapter 7 covers organizational aspects concerning "Security Assessment, Analysis and Assurance". A system security process is defined and described in detail. Since there is no information that needs to be up-to-date because of the content being so high-leveled, this chapter enables the reader to get a quick overview about the relevant content. The only thing that could be complained about is, that there are no references to the industrial standards and frameworks which are providing a lot of support during the definition, implementation and monitoring of these processes.[5]

[1] With their "service provider": botnet herder, harvester, mailer, coder, money-mule, etc. and their offered services like: classic spam, stock spam, pharming, phishing, SMiShing, redirecting, adware, tracker, ...

[2] Although sometimes I was wondering about the structure of the chapters: for example, if there is a section, like 8.6 and a subsection, like 8.6.1, I was certainly expecting a following subsection like 8.6.2 – but it never came.

[3] Bless et al. 2005 – Roland Bless, Erik-Oliver Bla, Michael Conrad, Hans-Joachim Hof, Kendy Kutzner, Stefan Mink, Marcus Schöller: Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen; Springer-Verlag 2005; ISBN 3540218459.

[4] Wang 2009 – Jie Wang: Computer Network Security, Springer-Verlag 2009, ISBN 3540796975.

[5] For example, there are CobiT (Control Objectives for Information and Related Technology), ITIL (Information Technology Infrastructure Library), ISO 27001/2 (covers requirements to Information Security Management Systems).

2.2 Part III: Dealing with Network Security Challenges

"Disaster Management" is presented in chapter 8. After the description of different kinds of disaster-categories, the prevention, response and recovery are discussed. This chapter seems not very network specific highlighting again the problem, that sometimes the focus of the book gets lost procuring the impression that recent papers are just plugged together to fill the content. Finally, some tips and tricks for companies are given, which also disregard some important technologies like backup technologies using the "Cloud", for example.[6]

The following chapter 9 is about "Access Control and Authorization", the 10$^{\text{th}}$ about "Authentication". They will be reviewed together with the result to give a complete overview about the contents you have to really think about, if you want to implement a practical network security. Mentioned topics are different access control techniques and technologies as well as access control systems. The relevant authorizations mechanisms and systems are explained with the final focus on granularity and web accesses. The areas of segregation of duties and the principle of least privilege are covered, too. Based on this background the following authentication methods can easily be understood. After introducing the authentication elements the two types of authentication (nonrepudiable/repudiable) are explained and the different authentication methods are presented. The last content covers the authentication policy, where the key points are accentuated in a accurate way. The only one thing to complain about is the reference on page 215, where the RFC 1760 is referred to, which is based on MD4 and MD5 encryption algorithms. Since 1996, the MD4 mechanisms is considered to be broken – this weakness should be mentioned.[7]

The next chapter 11 "Cryptography" is a core chapter because of covering the mandatory requirements to ensure a *secure* network environment (including transferring and storing data). After introducing the different kinds of block ciphers the principles of symmetric encryption are described. The example of DES remains a little bit unclear to the reader. Although it is mentioned that DES is no longer considered as secure, the argumentation, that "3DES is complicated and complex, and therefore secure" is questionable. Have you ever heard about Kerckhoff's principle?[8] Also the figure 11.3 referred to explain the 3DES concepts only shows the methods of single DES. Perhaps it would be helpful to the reader to point out, that 3DES is based on the principles of DES and uses a "key bundle" which comprises of three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm then would be: ciphertext = $E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$.

In the following the public key encryption is described on very basic level. It is rather incomplete since it only mentions one scheme by Diffie-Hellmann. There should be a more precise explanation. Btw., it is not understandable, why the author quite often talks about "Diffie-Halmann"...[9] First, their should be an introduction on underlying problems (like integer factorization, discrete logarithm or elliptic curves), then why it is secure and how to rate an algorithm with regard to the company-specific requirements (concerning the network security). The chapter is finalized with an overview about key management procedures and public key infrastructures, where some keywords like "web of trusts" with the classical example of PGP are missing. The concluding content covers hash functions and digital signatures and gives a short overview about their features and why to use them. Since the two latter only cover two and a half pages, the topics mentioned are not discussed in depth.

Chapter 12 "Firewalls" refers to different types, configuration and implementation of firewalls. This area of research is almost completely investigated, despite only a few points are missing. To get a complete overview, one should have a an additional look at application layer gateway technologies and the virtualization of firewall components. The following chapter 13 "System Intrusion Detection and Prevention" gives a basic understanding of the working of intrusion detection tools like NIDs and HIDs[10] with a side view to the consequences resulting out of an incident and the implementation of a company-

[6] Some chapters have even colloquial section titles like: "Always be ready for a disaster" (# 8.5.1, p. 182) or "Always backup media" (# 8.5.2, p. 182).

[7] As reference, there a lots of papers available about the collision-attack on MD4 hash values; http://eprint.iacr.org/2005/151 or http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.1448.

[8] "A cryptosystem should be designed to be secure if everything is known about it except the key information."

[9] I also googled the word "Diffie-Halmann" but their where only three hits.

[10] Network-Based Intrusion Detection Systems and Host-Based Intrusion Detection Systems

wide intrusion detection system as well as an intrusion prevention system. In addition to this the respective benefits are identified, referring to the corresponding papers.

"Computer and Network Forensics" is described in chapter 14. It is divided in computer and network forensics and the corresponding tools. The figures presented in the whole chapter lack a little bit of up-to-dateness as mentioned before. The main concepts are the same and for current data evaluation, the relevant sources and citations are given. In my point of view, the historic overview and the side-information is not necessary as well as bioforensics is not mandatory, too. But there is one subsection in this chapter comprising valuable checklists and How-Tos covering the main points to focus on if you really have to do forensic activities. In addition to this, there are lots of tools referred to as being useful for different steps of an analysis. However, some of the tools presented no longer exist any more. But as a general rule there are lots of tips and hints given on how to successfully conduct a forensic audit of either computer or network analysis although there are some redundant contents compared to previous "IDS/IPS"-chapter no. 13. Conclusion: thumbsup.

The 15$^{\text{th}}$ chapter covers "Virus and Content Filtering". This chapter gives mainly a historic overview about the different virus technologies and the associated scanning and detection technologies. Since this chapter has received its last update in 2003 (referring to the years used in the citations) it seems a little bit outdated again. But, as already said, it gives a nice historic overview. In my opinion, topics like scareware, drive-by-downloads, an so on should be mentioned and the chapter should directly be associated to the ones[11] referring to technologies like malicious code on websites (frame-jacking, compromised flash-data or interactive forms) or embedded code in PDF-files[12]. The advanced exercises in this chapter are very demanding, because in one of them you have to write an anti-virus code for a randomly chosen virus – against the background of polymorphic viruses and perhaps the ones which are distributed over the net with the ability to reload necessary attributes it would be very hard to do so. Also, the challenge to prepare a complete list of all viruses "in the wild" or to give a comprehensive list seems to be unfeasible (but I wish you "Good Luck! " if you really want to do it).

The following chapter 16 presents "Standardization and Security Criteria: Security Evaluation of Computer Products". In my humble opinion, the topics mentioned here are a little bit out of scope since the book wants to be a guide to network security. Sure, it is nice to know that there are different organizations which published their own frameworks and regulations, but why is the main ISO/IEC standard on IT network security not referred to (ISO/IEC 27033-{1, 2, 3}:2009[13])? The other content covers the security evaluation criteria through the "CC (common criteria)", the "Orange Book" or the ITSEC (Information Technology Security Evaluation Criteria). It is a pity that the authors asks some interesting questions only in the context of the exercises without giving the answer (for example regarding to the meaning of being compliant to the CC or to ISO).

The interesting topic of "Computer Network Security Protocols" is covered in chapter 17. Expecting group communication protocols, encryption, authentication, revocation, performance, security-features and things like that, the reader only gets an overview about the fundamental ones, particularly there are the ones covered which are used within the application level, the transport level, the network level and the link level. But back to basics – since it is a book for undergraduates, the topics mentioned are suitable for the target group. Since the technologies are still used, there is no need to update them – only if there security features being no longer valid. This is the case of Kerberos. In the text (for example in table 17.2) Kerberos 4 is named; there should be a warning of using this option because it is not secure anymore. Since 2005 the IETF Kerberos working group is updating the specifications.[14] The next confusing thing is figure 17.2. If you are familiar within the Greek myths, the so called "cerberus" is a three-headed hound which guards the gates of Hades – and so you would expect three communicating parties. Unfortunately, there are only two (user and authentication server). To clear it up, there should be in addition to them a TGS (ticket granting server) like mentioned in the text. The following security

[11] Such as chapter 5 "Cyber Crime and Hackers" on page 107 as well as chapter 6 "Hostile Scripts" on page 133.

[12] It mostly uses exploitable bugs in the Acrobat Reader – for example, there exist viruses using payload: http://www.f-secure.com/v-descs/exploit_w32_pdf-payload_gen.shtml.

[13] IT network security framework, a multi-part standard based on ISO/IEC 18028:2006.

[14] See RFC 4120, http://tools.ietf.org/html/rfc4120 or RFC 4121, http://tools.ietf.org/html/rfc4121.

in the transport layer is based on the description of SSL (secure socket layer) and TLS (transport layer security). IPSec (Internet Protocol Security) and VPNs (Virtual Private Networks) are described in the chapter about the network layer security. Some information is presented twice with the tunnel modes and the VPN technology being already presented in the "Firewalls" chapter (page 249 ff.). The chapter is finalized with the security in the link layer and over LANs. Extended information about the RADIUS (page 220) is given and the already known structure of each chapter is followed by giving the basic exercises and the advanced ones.

Chapter 18 and 19 cover "Security in Wireless Networks and Devices" as well as "Security in Sensor Networks". Since both chapters being not very common a lot of the space being available (two-thirds) is used for explaining the technical details and presenting some protocols and technologies in use. As a result, the focus an security-relevant aspects covers only a quick overview about some attacks and, in conclusion of them, some best practices for Wi-Fi security. Still outdated information is presented: WEP is considered as secure and there is no word about the current standards like WPA2 with the AES-based IEEE 802.11a, b, g or n.[15] The following chapter about sensor networks is very interesting. Although it is one of the shortest chapters with about 10 pages, there are the most references available really giving a state of the art overview! A good introduction is given and an easy understanding of the technologies and threads is reached.

The last two chapters cover "Other Efforts to Secure Information and Computer Networks" (chapter 20) and "Security Beyond Computer Networks: Information Assurance" (chapter 21) and focus explicitly on organizational and economic aspects. Therefore topics like legislation, regulation, self-regulation, education, reporting centers, market forces and activism are presented in a simplified way. And, well, the last chapter talks about national security initiatives and awareness as well as training programs. To sum it up, the two chapters, no. 20 and 21, could be skipped – in my humble opinion.

3 Recommendation

I think, that the book is only suitable for scientific uses during courses for undergraduates. Since the book covers lots of aspects it gives a quick overview about lots of technical, historical and organizational contents and is therefore useful for practitioners. Because there is no mathematical explanation of details in protocols or cryptographic procedures, you can easily handle the topics mentioned and get a fine grasp. Unfortunately, many of the themes lack of being up-to-date, because of the newest citations being from 2002/2003. To sum it up, there is only limited use for academic research but for practitioners and self-studies enough information is given without describing the topics in detail.

One last thing to mention is chapter 22 which covers various kinds of research projects available for different time periods (consisting of "Weekly/Biweekly Laboratory Assignments", "Semester Projects" and concrete "Research Projects"). This chapter deals with topics that open up perspectives beyond the ordinary and is a really nice additional feature compared to the rest of the book.

The reviewer works as an IT-auditor in Germany.

[15] See http://standards.ieee.org/getieee802/802.11.html.