Review of the book

”Security for Telecommunications Networks”

by Traynor Patrick, McDaniel Patrick and La Porta Thomas

Springer Advances in Information Security, Vol. 40, 2008

ISBN: 978-0-387-72442-3

Nishant Doshi
MEFGI, Gauridad Campus, India

1 Summary of the review

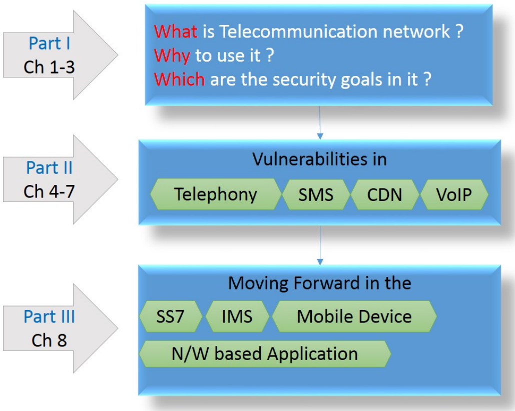
One thing I like about this book is the way of organization in 3 parts. And also the technical depth in introduction (part I) is well enough to digest the remaining portions in the book. In this book, chapter and subsequent chapters, I like the way authors have used the footnoted to give important historical aspects as well as to pinpoint the link to the section in part I for sharpen the fundamentals. It suggests the researchers to study the analysis & simulations part for how to do analysis of the given scheme. This book is broadly (and nicely too) divided in *three* parts as in the Figure.

2 Summary of the book

Chapter 1 In general, preface is written in starting of each book to show the outline of the book, while this book follows the approach as in research papers i.e. writing it as the subsection in the introduction. This chapter starts with the motivation for writing this book and afterwards explain (in brief) the telecommunication network, its convergence and security. In this chapter, I specially like subsection 1.4 that says about the intended audience to read which chapter for specific background.

Chapter 2 This chapter fruitfully considers the basic terminology for the audience who are not familiar with *what* is security, cryptography, authentication, etc. I welcomed the authors to cover the required information on security for this book as in this form.

Chapter 3 This is the last but important chapter in part I of the journey. This chapter explains the history of cellular networks and its system architecture.



Chapter 4 This chapter discusses the security issues and findings in the cellular networks. It start with the analysis and vulnerability of COMP128 that used in industry. Afterwards, it explains the vulnerabilities in the telecommunication network with the example to AT & T network. Also, it explains the eavesdropping and jamming in the wireless network. Finally, it shows how the user tracking and privacy, malware etc. can affects the data networks.

Chapter 5 SMS (Short Message Service), the technology that have major impact on our daily life as it now. This chapter start with historical findings of SMS, how your SMS delivered to destination, how it routs its path in the wireless. After this, the authors have nicely turn the attention to the limitations or vulnerabilities in this system through queue management, denial of service, network and attack characterization. Finally, it states the current solutions (with assumptions) in the denial attacks, queue management. Authors have nicely organized & analyzed the different message bandwidth techniques.

Chapter 6 One nice point about this part II is that it follows same gadget for each chapters i.e. historical findings, mechanism, security analysis and way to dealt with it. This chapter discuss about data networks of high speed as to that of SMS. It discusses the GPRS and GSM network with their setup in real time scenario. It also discuss the implication of varying setup & network mechanism affects the analysis. Surely each of chapter in part II is a kick start for researchers to think and get the further directions.

Chapter 7 This chapter discusses the VoIP (Voice over IP). As in previous chapters, this chapter start with historical background and evolvement of present architectures from it. The authors have explored the SIP protocol of VoIP, its mechanism and solutions (as identified in research) is discussed with further direction for secure IP telephony networks.

Chapter 8 This final part/chapter talks about the future challenges, future directions in different security protocols.

3 Comments and Recommendations

I suggest to considers the example scenario and how the vulnerabilities in it can be exploited. Also, some tools by which one can do such kind of analysis and it also handful for the students and the researchers. This book is the bridge for students to learn about what is security, vulnerability and how to exploit it, thus from study to the research. For the researchers, this book gives the fundamentals understanding of the topics. Also, vulnerability analysis and most importantly the part III- i.e. research areas in the current field of cellular networks. I recommend this book to the UG students to strengthen their fundamentals on telecommunication network and security. For the PG student (and researchers too) to get the well depth understanding with further scope of improvements in the security aspect of cellular networks. As some portions in this book requires knowledge of some mathematical terms. It will be beneficial to add appendix for quick introduction of this terms.

On an average, this book gives the undergraduate students (of final year), postgraduate students, researchers, scientists and so on to motivate and also to study further in the security in communication network. Surely, I suggest this book as first hand book for UG, PG and the researchers.

The reviewer is a faculty at MEFGI, India.