Book Reviews

Mike Hendry

Smart Card Security and Applications

Artech House, Inc., 685 Canton Street,
Norwood, MA 02062, ISBN 1-58053-156-3

Different types of plastic cards have been around for decades. They are used in variety of applications such as traveling, telephony, identification, cash obtaining and all sorts of payment. Plastic cards were introduced in America as credit cards; at first just plain plastic with simple pattern, but rapidly evolving, discovering new applications and adding new features. Offered by different issuers for different applications, cards became inevitable in almost any part of the world, from industrial Western countries to the Far East.

Plain plastic cards were soon replaced with magnetic stripe cards, and finally 70s brought invention of smart card. At first, growth in use was insignificant, but since the 90s smart card market is growing fast.

Since smart cards (and other cards) are used for security and financial purposes it is crucial to incorporate different security measures from built-in security to issuing a use policy in order to minimize threats of misuse, fraud, counterfeits and other security breaches.

This book introduces reader to smart card use and security, covering topics from smart card technology, security and applications. The book is divided in three sections each covering some of the aspects mentioned before.

The first section brings the reader into a problem, describing the background issues. It covers and explains security topics such as authentication, confidentiality, integrity, nonrepudiation and reliability, breaking them down and relating them to real world needs. This section also explains different threats, incidents, causes and modes of failure as well as risk management, standards and specifications.

The second section explores smart card technology from bottom up, starting with basics and history, introducing also magnetic stripe, optical and IC cards. Next chapter is dealing with encryption terms, describing symmetric and asymmetric key algorithms, keys and key management. Usage of passwords and biometrics is explained in chapter 6. Chapter 7 distinguishes smart card types and characteristics, explaining memory and microprocessor card types, as well as contact, contactless and some other form cards. Next chapter is dealing with chip card security, explaining security features, possible attacks and countermeasures. Remainder of this section presents multiapplication operating systems, functions and products. Moreover it covers other system components such as smart card readers, terminals and networks, as well as basic processes and procedures form chip design, manufacture and personalization to issuance, card usage and procedures required for lost, stolen or misused cards.

Last section covers different smart card applications. Chapter 12 deals with telephony and broadcasting applications, explaining smart card usage in fixed and mobile telephony, also covering usage in cable and satellite television. Other smart card applications, which will grow rapidly in future, is its usage in computer networks and E-commerce, which is described in chapter 13. Next chapter presents financial applications which happen to be among the most important, but also the most delicate. It covers bank cards, credit and debit cards as well as electronic purses and on-line transactions. The following chapters describe smart card usage in health and transport, also covering private identification applications, explaining different approaches and problems. Finally, the last section gives a brief look into commercial structures for multiapplication cards, designed for security and some future forecasts.

This book introduces the reader to smart card technology, security and its applications. It provides technical details about card types, important security issues and today's applications in telephony, finance, health, transportation, also giving future perspectives of the development in all the aspects. The book does not explain in-depth any of the standards, procedures, security methods or applications, it rather gives a brief overview of all the aspects necessary to understand smart card technology, providing potential readers with a general look into all the important topics, with references to additional literature needed for deeper understanding of the specific issue.

Hrvoje Šegudović
Faculty of Electrical Engineering
and Computing
University of Zagreb
Croatia

Sheila Frankel

Demystifying the IPsec Puzzle

Artech House, Inc., 685 Canton Street,
Norwood, MA 02062, ISBN 1-58053-079-6

IPsec, the suite of protocols for securing any sort of traffic that moves over an Internet Protocol (IP) network, promises to be the main thing for online business. Demystifying the IPsec puzzle tries to go into specifications that compose this suite of protocols and to explain how they fit into the Internet, Virtual Private Networks and online business. Every feature and even future possibilities of IPsec are systematically described in this book.

Organization of the book is pretty straightforward. Twelve chapters describe all of the IPsec features of which some are already implemented but others are still being discussed about. The first chapter sets a common ground for understanding IPsec by introducing its underlying framework, the TCP/IP networking suite. IP version 4 and 6 packet structures and addressing schemes are explained.

In the following chapters, basics of IPsec are explained. As IPsec attempts to enable security protection by the use of two optional headers, Authentication Header (AH) and Encapsulation Security Payload header (ESP), format of those headers, as well as their processing, is explained into great detail. Processing of both inbound and outbound messages that use AH or ESP headers is constructed step by step. After AH and ESP headers structure is clear enough, the following chapter explains cryptographic algorithms that are used to afford IPsec protection. MD5, SHA-1 and HMAC algorithms are showed step by step again, but maybe on a too high level for more technical readers. However, for a less technical reader, description of DES and 3-DES algorithms is very good.

In the next, fifth, chapter, the Internet Key Exchange (IKE) protocol is explained. As IKE is a very complex protocol, much space is dedicated to the explanation of messages flow during the negotiation between initiator and responder host. Pluses and minuses of this protocol are stated, as well as possible directions in future development, as IKE is still actively being developed at the time of writing book and this article. Also, maybe more explanations and examples could help readers to easier understand the mechanism of the IKE.

After the common ground for IKE understanding is set, the author goes more deeply into real world examples of IKE use. In the following chapter different authentication methods which can be used with IKE are presented. This chapter is especially interesting for today's use, as there is increasing popularity of telecommuting. With this use, the author also presents different add-ons to IKE protocol. For more technical readers, PF_KEY API is explained as the main interoperability tool between IKE and IPsec implementations.

At the end, policy setting and enforcement are discussed into detail. A reader can see that a lot of work still has to be done in this field. Also, basics of the Public Key Infrastructure (PKI) are presented in this chapter, as well as potential problems of secure IP multicast protocols.

This book gives to potential reader excellent overview of IPsec possibilities and directions in future development. However, sometimes it lacks real world examples and technical details about implementation. Also, sometimes the book is pretty hard to read. The grammar and sentence structure aren't bad but they can be hard to follow — and the text doesn't flow smoothly.

Bojan Ždrnja
Faculty of Electrical Engineering
and Computing
University of Zagreb
Croatia

John E. Canavan

Fundamentals of Network Security

Artech House, 2001, ISBN 1-58053-176-8

There is respectable number of "security" books out on the market today. But most of them deal with some specific area like encryption, firewalls, DoS attacks etc. On the contrary, this book tries to cover the whole area. Pretty ambitious, but the author nicely positions this book in his preface, clearly declaring it as entry level guide to security beginners. But, computer and network security are such an important and complex field that it can be hardly entered by reading any one book. Entry level security engineers are usually specific area experts, Unix experts or firewall experts, for example. And that is often their main problem, because they lack the security "big picture". Can this book provide it to them?

In opening chapters, the author explains why is security needed and counts most usual threats. One could argue if he overestimates potential damages, but he clearly points out that security implementation costs and also affects network and system performances, which some authors tend to dissemble. He also correctly says that there is no absolute security. In threats explanation author doesn't go in technical details at all, and that is the biggest problem of such a wide-area book — to find a good balance. There is also a list of useful Web sites — security sites, but also hackers' sites. Good starting point for finding more information.

Next few chapters are dedicated to data encryption, certificate authorities, digital signatures and key exchange systems.

In Chapter 6, the author deals with e-mail security. He deals mostly with confidentiality and integrity of messages and nicely describes methods for encryption and secure storage.

The next chapter discusses operating systems security, providing detailed description of system security for most usual Unix and NT systems. Few useful tools for those systems are briefly analysed. LAN Security chapter also deals mostly with OS security and access rights. Only the method for traffic segmentation discussed in this chapter is using switches instead of hubs. These days VLANs and inter-VLAN security are hot topics but are not discussed here. It would be very useful to describe fundamental rules for network organisation and traffic flow direction, but the author mostly describes single station or OS security aspects. In general, the book lacks network organisation info and recommendations, which can be very important for every network connected to Internet.

In the next few chapters, media, protocols, Cisco IOS and SNMP security topics are described and discussed. Chapter 11 brings another hot topic — VPNs. But, this chapter shows best how hard it is to write a book covering such a wide area. Dealing with details can bring mistakes. The author says, for example, that for end to end L2TP (Layer 2 Tunnelling Protocol) implementation — all nodes must be L2TP compliant. Very wrong and pointless.

Chapter 12 introduces Firewalls. They are correctly categorised and described, but most advanced firewall possibilities are not pointed. Today, firewalls can be more than perimeter defence. They can detect DDoS attacks, generate real-time alarms and reports, and integrate with antivirus and content filtering tools. And, they can even provide security implementations between internal networks (VLANs) and users. In Chapter 13 — biometric identification and authentication are described. Chapter 14 emphasises the importance of appropriate security policies, as security base, and their implementation through more specific and detailed procedures. Next chapter describes some advanced security systems like Intrusion Detection Systems, which can be very useful, but also expensive and hard to implement and maintain.

Chapter 16 recommends what to do and how to prepare for possible security crisis. Many organisations don't have such a plan and if attack happens they won't be ready to alleviate the damage. In the last chapter, some common threats related to Web are described. Cookies, cache, Java scripts are discussed as potential threats to hosting systems.

This book tends to cover really wide aspects of computer and network security. Although the author declares it as entry level book, he finds it difficult to achieve good balance between global descriptions and the depth of technical detail. It led him to some technical mistakes. One can also discuss if this book covers all the areas it tends to. For example, network organisation and segmentation is hardly touched and antivirus security is not systematically exposed and solutions are not proposed. In spite of that, this book is very useful as a reference point for most security areas. The reader can get the "big picture" of network security issue. He can't learn some specific topics in detail, but he can start from here. The book can be useful even to some specific security area experts who need to widen their knowledge. And it can be also useful for experienced IT personnel and managers responsible for organising the whole security policy for their organisations.

Boris Obradov
Faculty of Electrical Engineering
and Computing
University of Zagreb
Croatia

Data Mining: Technologies, Techniques, Tools, and Trends

Thuraisingham B. Boca Raton, FL: CRC Press, 1999, ISBN 0-8493-1815-7, 270 pp., $64.95

Focusing on a data-centric perspective, this book provides a comprehensive overview of data mining on almost all aspects, including its basic concepts, current technologies, popular techniques, commercial products, and future challenges. Since it is written for technical managers and executives as well as technologists interested but inexperienced in data mining, this book is provided with plentiful diagrams that help readers quickly grasp the complex meanings of technical texts.

The book is divided into three parts:

Part I describes technologies for data mining, including database systems, data warehousing, statistical reasoning, machine learning, visualization, decision support, parallel processing, and architectural support for data mining. Since the author believes that having good data is key to mining, technologies other than data management are just briefly introduced. However, this deficiency is well offset by an abundant reference list and two appendices providing additional information on data management and artificial intelligence technologies at the end of this book.

Part II presents tools and techniques, including getting the data ready, carrying out the mining, pruning the results, evaluating outcomes, defining specific approaches, and citing research prototypes and commercial products for up-to-date information. What should be mentioned is, that due to the author's research interest and the belief that ILP may play an important role in building theoretical basis of data mining, Logic Programming occupies a full chapter of this book. However, it is a pity that some famous software such as Business Object Co.'s Business Miner TM is not cited in the chapter presenting commercial products.

Part III that occupies nearly half length of this book is instructive even to expert researchers. It presents possible solutions for emerging trends, including mining distributed, heterogeneous and legacy data sources, mining multimedia data, mining data on the web, metadata aspects of mining, security and privacy issues. Moreover, several other areas that need further work are indicated in the last chapter, including data understanding, incomplete and uncertain data, multilingual mining, multi-strategy learning, scalability, as well as better data mining techniques, theory of data mining, and integration of technologies. What should be mentioned is that the author says there is no clear difference between mining and information retrieval when multimedia data is dealt with. However, I believe that although those two technologies are really very overlapped, in some cases they can be distinguished in two aspects. First, the goal of mining is decision support while that of information retrieval is more flexible. Second, users should have some knowledge on the information they want to retrieve, no matter how vague the knowledge is; while they may have no opinion about what they can get from mining. For example, “show me the scenes where Bob appears in this video” is an information retrieval task; while “analyze this video and give me some advice on how to promote our sales” is a mining task.

All in all, this book is a good introductory material especially helpful to business managers and project leaders who want to profit from the goldmine of data mining. Before rushing into this area, they had better answer the questions stressed in this book: Is there a need for mining? Do you have the right data in the right form? Do you have the right tools? More importantly, do you have the people to do the work? Do you have sufficient funds allocated to the project?

Zhi-Hua Zhou
National Laboratory for Novel Software
Technology, Nanjing University
Nanjing 210093, P.R. China
e-mail: zhouzh@nju.edu.cn