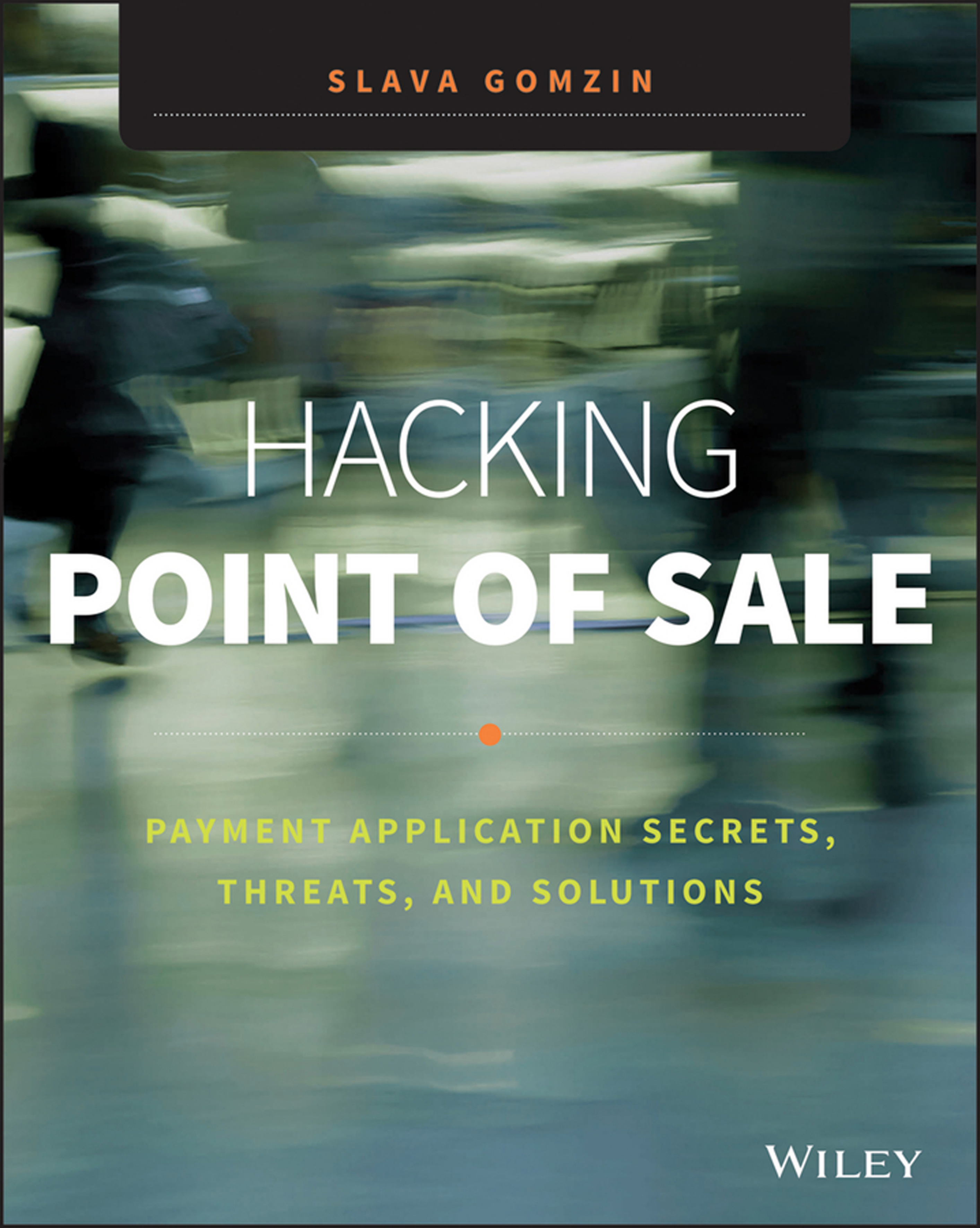

SLAVA GOMZIN

# HACKING POINT OF SALE

PAYMENT APPLICATION SECRETS, THREATS, AND SOLUTIONS

WILEY

# Hacking Point of Sale

# Hacking Point of Sale

## Payment Application Secrets, Threats, and Solutions

Slava Gomzin

WILEY

**Hacking Point of Sale: Payment Application Secrets, Threats, and Solutions**

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

ISBN: 978-1-118-81011-8
ISBN: 978-1-118-81010-1 (ebk)
ISBN: 978-1-118-81007-1 (ebk)

Manufactured in the United States of America
10 9 8 7 6 5 4 3 2 1

**Limit of Liability/Disclaimer of Warranty:** The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

**Library of Congress Control Number:** 2013954096

*To all of us who pay and get paid with plastic.*

# About the Author

**Slava Gomzin** is a Security and Payments Technologist at Hewlett-Packard, where he helps create products that are integrated into modern payment processing ecosystems using the latest security and payments technologies. Prior to joining Hewlett-Packard, Slava was a security architect, corporate product security officer, R & D and application security manager, and development team leader at Retalix, a Division of NCR Retail. As PCI ISA, he focused on security and PA-DSS, PCI DSS, and PCI P2PE compliance of POS systems, payment applications, and gateways. Before moving into security, Slava worked in R & D on design and implementation of new products including next-generation POS systems and various interfaces to payment gateways and processors. He currently holds CISSP, PCIP, ECSP, and Security+ certifications. Slava blogs about payment and technology security at `www.gomzin.com`.

# About the Technical Editor

**Rob Shimonski** (`www.shimonski.com`) is an experienced entrepreneur and an active participant in the business community. Rob is a best-selling author and editor with over 15 years of experience developing, producing, and distributing print media in the form of books, magazines, and periodicals. To date, Rob has successfully created over 100 books that are currently in circulation. Rob has worked for countless companies including CompTIA, Wiley, Microsoft, McGraw-Hill Education, Elsevier, Cisco, the National Security Agency, and Digidesign. Rob has over 20 years of experience working in IT, networking, systems, and security. He is a veteran of the U.S. military and has been entrenched in security topics for his entire professional career. Rob has an extremely diverse background in security and networking and has successfully helped over a dozen major companies get on track with PCI.

# Credits

**Executive Editor**
Carol Long

**Senior Project Editor**
Adaobi Obi Tulton

**Technical Editor**
Rob Shimonski

**Production Editor**
Daniel Scribner

**Copy Editor**
Christina Haviland

**Editorial Manager**
Mary Beth Wakefield

**Freelancer Editorial Manager**
Rosemarie Graham

**Associate Director of Marketing**
David Mayhew

**Marketing Manager**
Ashley Zurcher

**Business Manager**
Amy Knies

**Vice President and Executive Group Publisher**
Richard Swadley

**Associate Publisher**
Jim Minatel

**Project Coordinator, Cover**
Katie Crocker

**Proofreader**
Sarah Kaikini, Word One

**Indexer**
Robert Swanson

**Cover Designer**
Ryan Sneed/Wiley

**Cover Image**
© defun/iStockphoto.com

# Acknowledgments

First, I would like to thank Wiley for providing me with this unique authorship opportunity. Thanks to my editor, Adaobi Obi Tulton, for her patience, attention, and support throughout the entire publishing process. Special thanks to Carol Long who believed in this book and made it possible. Thanks also to my first editor, Jeannette de Beauvoir, who helped me to polish and promote my book proposal.

Writing a book like this wouldn't be possible without gaining experience and learning from other professionals over the years. I would like to thank my former coworkers. Special thanks to Shmuel Witman, Doug McClellan, Sagi Zagagi, and Ofer Nimtsovich, who influenced me at different stages of my career by sharing their knowledge and vision, and helped me to survive in this industry and develop myself professionally.

Finally, special credit goes to my wife, Svetlana, and my daughters, Alona, Aliza, and Arina, for understanding the reasons for my absence from their lives on countless weekends and evenings while I was working on this book.

# Contents at a Glance

# Contents

# Introduction

***False facts are highly injurious to the progress of science, for they often long endure; but false views, if supported by some evidence, do little harm, as everyone takes a salutary pleasure in providing their falseness; and when this is done, one path towards error is closed and the road to truth is often at the same time opened.***

**—Charles Darwin**

Nearly five million point-of-sale (POS) terminals process about 1,500 credit and debit card transactions every second in the United States alone.[1, 2, 3] Most of these systems, regardless of their formal compliance with industry security standards, potentially expose millions of credit card records—including those being processed in memory, transmitted between internal servers, sent for authorization or settlement, and accumulated on hard drives. This sensitive data is often weakly protected or not protected at all. It is just a matter of time before someone comes along and takes it away. Valuable cardholder information can be stolen from many places in a merchant's POS system, such as unprotected memory, unencrypted network transmission, poorly encrypted disk storage, card reader interface, or compromised pinpad device.

There are more than one billion active credit and debit card accounts in the United States.[4] It is not surprising that such cards have become an attractive target for hackers. In 2011, payment card information was involved in 48% of security breaches—more than any other data type.[5] In 2012, POS terminals and payment data were record breakers in three different categories: The variety of compromised assets, the variety of compromised data, and the breach count by data variety.[6]

Information about breaches and new types of malware aimed specifically at payment systems is popping up in the mass media almost every day, and yet we're seeing only the tip of the iceberg since many incidents aren't reported to the public. In such a critical situation, it's very important to assess the balance of power between offensive and defensive sides in order to decide what to do next.

PCI standards provide a great security baseline, but they still don't protect electronic payments adequately. Once merchants and software vendors achieve

PCI compliance, they should continue securing their systems beyond the basics in order to reach a reasonable level of protection.

This book summarizes, systemizes, and shares knowledge about payment application security. All the aspects of card payment processing—from the structure of magnetic stripe to architecture and deployment models to communication protocols— are reviewed from the security viewpoint. Usually, information security takes care of three major subjects: confidentiality, integrity, and availability. All three are very important. When we talk about security of payment applications, all three subjects are still applicable: the payment data should be protected from disclosure at all times, it should not be altered, and the payment service should be ready to use 100% of the time. However, as we know, the greatest threat related to electronic payments is stealing sensitive authentication data, specifically Track 1, Track 2, or PAN. Therefore, payment application security is naturally focused on the first information security principle, confidentiality, and its associated threat, information disclosure. This fact explains why security standards related to payments, such as PCI, primarily talk about controls which take care of confidentiality.

Speaking of POS and electronic payments, we certainly are not thinking of just traditional brick and mortar stores. Online payments are another huge field which probably deserves no less attention. Since both of these areas are equally huge, they would not fit properly into the framework of a single book. Discussion about online payments requires at least an overview of special topics such as security of data centers and, obviously, web application security. At the same time, some very important subjects, such as POI devices, are not applicable when talking about e-commerce security. This book is dedicated to in-store payment systems and all the aspects of their security. Perhaps online payments will be a great topic for my next book.

Before we dive into the details of vulnerabilities and attack vectors, let's define the scope of the threats. It is important to understand that while we are talking about threats to POS systems, most of the attacks are performed on *payment applications* which can be either an internal part of the POS system or a completely separate module. Payment application is a desired target because in most cases it is a piece of software running under a Windows operating system on PC-based devices connected to a local network or even directly to the Internet. In combination with the fact that it accepts, processes, stores, and transmits sensitive payment card information, this opens various possibilities to steal the money remotely. From this point forward when we say "point of sale" it means "payment application" and vice versa.

## Author's Note

In the spring of 2011, I was urgently called to my then employer's corporate headquarters in Israel to work on a special project. I was asked to lead the design and development of a new payment system for one of the largest supermarket chains in Europe (name withheld for privacy). I had been working full time on security and PCI compliance rather than development, but my 10 years of experience in the development of payment interfaces gave them some hope of saving the project after several previous failures. I was given substantial resources, but the schedule was very tight for a project of such magnitude: we had two months to release a working version. In addition, the solution needed to be designed using the latest technology and security standards.

The development team I was given was made up of the best possible programmers. Almost immediately, however, I ran into an unexpected problem: Since the product was new, no one in the group had a clue about payment interfaces—despite the fact that they already had experience in POS development. Of course, there was no question about security or PCI compliance.

The first few days and even weeks were spent explaining electronic payments in general, the details of the architecture of payment applications, and security standards in this area. Everyone knew what a credit card was and how to swipe it, but that was it! I thought it would be useful to have a guide to introduce new architects and programmers to the field, but I knew that such a guide didn't exist. My own knowledge in this area was accumulated through many years of work on a variety of payment systems and studying the application security. That's when the idea for this book was born.

Eventually, the payment solution was successfully delivered on time and I returned to the United States to continue with my regular job. But I couldn't stop thinking about the book. Since then, the idea was slightly transformed to reflect the latest developments in the industry. For example, the widespread introduction of PCI standards has led to a shift in attack vectors, from data storage to memory. Also, newborn P2PE standards brought high hopes for merchants and great challenges for software developers and hardware manufacturers. However, the essential goal remained the same: Create a guide for developers, security professionals, users of payment systems, and executives, to help them understand the incredible blending of architecture principles, industry standards, software vulnerabilities, attack vectors, and cryptographic techniques that together make up payment application security.

## Who This Book Is For

There are several types of users that will benefit from reading and using the information in this book.

*Point of Sale and Payment Application Developers*, *Development Managers*, and *Software Architects* working for software vendors and service providers will learn the basics of payment applications and how to protect their products from security threats. There are a few code samples provided for this group at the end of the book. (I know, hackers do not code in C#, but they know to translate it to C when needed.)

*QA Analysts* and *Managers* will get some ideas on how to create and conduct security penetration testing of payment software.

*Security Architects*, *Managers*, *Consultants*, and *Executives* working for merchants will learn what questions they should ask payment application vendors and service providers in order to determine the level of protection of their software and hardware.

*Solutions Architects*, *Project* and *Product Managers*, and *Executives* working for both vendors and merchants will learn about areas of potential vulnerabilities in order to be able to estimate the risks associated with implementing payment solutions and efforts necessary to mitigate them.

## Pros and Cons of Security Through Obscurity

I was thinking about this issue when I started writing the book and was noticing a significant amount of sensitive information I potentially disclose to "bad guys." I am sure there will be people asking "Why are you talking about these issues in the first place? We are putting so much effort into achieving PCI compliance, and you are saying it is not enough and showing how to hack PCI compliant applications! You are ruining our work! Let's keep these vulnerabilities secret until the PCI Council notices them, admits their importance, develops countermeasures, includes them into the next version of standards, and requires us to implement them!" Well, it sounds already too complicated to do in a reasonable period of time. And what if the bad guys already learned some of this stuff? They won't tell you about their knowledge. They will also keep it secret until the day they break your system.

There are two "clubs" in this game—hackers and developers. Both are closed clubs and both are trying to keep their secrets from each other. The problem begins when hackers become developers, or developers become hackers. In the first case, you get an “insider”—someone who knows your application’s secret tricks, back doors, and weaknesses. This information can be disclosed to third parties, or used directly by that person. In the second case, you have “secret” information that went with the person who left the company and was then free to use it or sell it to others. Both cases are bad if application security is mostly achieved through obscurity.

As Bruce Schneier said, “Disclosed vulnerability is one that—at least in most cases—is patched. And a patched vulnerability makes us all more secure. Minimize the number of secrets in your security system. To the extent that you can accomplish that, you increase the robustness of your security. To the extent you can’t, you increase its fragility. Obscuring system details is a separate decision from making your system secure regardless of publication; it depends on the availability of a community that can evaluate those details and the relative communities of “good guys” and “bad guys” that can make use of those details to secure other systems”.[7, 8] I am sure there is a community that is ready for this publication.

## What This Book Is Not

This book is not about payment card fraud protection. Those controls only protect the cardholder and the merchant before the card is swiped. However, they do not secure the sensitive cardholder data once it is entered into the system. Examples of such security measures are using CVV or ZIP code verification during authorization.

Although there is an entire chapter about PCI, as well as multiple references to the standards which became an essential part of the payment industry, this book is not a guide on PCI compliance. There are publications and training courses that will teach you about PCI. Rather, this book looks beyond PCI and provides practical recommendations on how to implement real application security controls. Neither is it about security of payment processing from the point of view of credit card brands. PCI standards help to secure only selected fragments of the big picture. However, the entire process, including implementation and deployment of payment applications, is vulnerable by design, and responsibility for its security is delegated to merchants, payment processors, software/hardware vendors, and service providers.

Security of payment processing data centers is also outside the scope of this book because it requires much more than just a single chapter. This book is focused on the retail store which is more vulnerable than any other electronic payment flow players.

## How This Book Is Structured

Good programmers follow coding conventions and best practices. One of the basic development principles is dividing the code into small, relatively independent pieces—several lines of code in size—which can be easily read and understood. The same approach was implemented in this book to minimize the size of each single section. The text is structured in a manner similar to professional technical documents, with a detailed table of contents that makes it simple to quickly locate and read specific pieces of information.

The book is divided into three main parts:

1. Technology overview
2. Description of attacks and vulnerabilities
3. Solutions for the problems (mitigations and protection measures)

**Part I, "Anatomy of Payment Application Vulnerabilities"** (Chapters 1, 2, and 3), sets the scene for Parts II and III by explaining the technological background of electronic payments. Even though it's an introduction to the world of cards and payment applications, all their components are reviewed from a security point of view.

**Chapter 1, "Processing Payment Transactions,"** covers the basics of payment processing: How different organizations—players in the plastic game—participate in the transaction flow, their responsibilities and challenges, and the differences between various payment transaction types, with detailed explanations of exception and error-handling scenarios.

**Chapter 2, "Payment Applications Architecture,"** introduces basic design concepts, compares different deployment models, and explains the main functional modules of payment application divided into two groups—interfaces and processors. It also explains the types of connectivity and differences between communication and message protocols.

**Chapter 3, "PCI,"** describes security standards that regulate the industry employing payment applications, and shows how they protect the sensitive cardholder data from being stolen. This chapter explains the difference between PCI DSS and PA-DSS from both merchant and software vendor perspectives. There is a description of standards (such as ISO and FIPS) that indirectly affect payment application security. The chapter introduces the PCI P2PE standard (the technical details of P2PE implementation are also explained in Chapter 8).

**Part II, "Attacks on Point-of-sale Systems"** (Chapters 4, 5, and 6 ) explains how card data can be stolen from POS machines, and why particular areas of payment applications are more vulnerable than others.

**Chapter 4, "Turning 40 Digits Into Gold,"** explains what is inside the payment card and how this knowledge helps the bad guys use stolen cards to get cash.

The goal of this chapter is to demonstrate the ease and simplicity of the credit card fraud by providing a step-by-step explanation of the process, from obtaining the "dump" to getting the cash. There's a detailed description of the carding that includes hidden and small but important tricks of encoding, embossing, and tipping fake cards.

**Chapter 5, "Penetrating Security Free Zones,"** describes payment application vulnerabilities not addressed by existing PCI security regulations. Although PCI defines a great security baseline, many areas of payment applications are covered by neither PCI nor other standards. This chapter also contains "bonus" sections about non-software attacks that are not directly related to payment applications but aimed at other areas of POS, such as the physical security of pinpad devices and design flaws in POS payment processes.

**Chapter 6, "Breaking into PCI-protected Areas,"** covers payment application vulnerabilities in areas that are supposed to be protected by current PCI security standards. Even though PCI standards require encryption on "data at rest," there are various vulnerabilities associated with data storage, such as weak encryption mechanisms and poor key management.

**Part III, "Defense"** (Chapters 7, 8, and 9), addresses the issues described in the previous part. It describes how to prevent attacks on payment applications by employing powerful cryptographic tools for protecting the cardholder data and payment application code.

**Chapter 7, "Cryptography in Payment Applications,"** explains the basics of cryptography in the context of payment application security, which provides necessary foundations for implementing protection controls defined in subsequent chapters. Information in this chapter includes a description of main cryptographic principles and applications such as symmetric and asymmetric encryption, digital signatures, and cryptographic standards. It provides the reader with knowledge needed for understanding and designing powerful protection mechanisms such as sensitive cardholder data encryption, digital signing, and point-to-point encryption.

**Chapter 8, "Protecting Cardholder Data,"** explains how the power of modern cryptography can be utilized in order to protect sensitive cardholder information from the moment of swiping the card at the POS to the transaction settlement. The chapter describes various methods of data encryption at any possible state—in memory, in transit, and at rest—including an introduction to the latest industry trend—a technology capable of protecting them all called point-to-point encryption. The chapter defines the different types of point-to-point encryption implementation—hardware, software, and hybrid—and how they affect security. It also explains the essentials of typical P2PE solutions such as DUKPT key management scheme.

**Chapter 9, "Securing Application Code,"** explains how to protect the payment application itself from attacks in the hazardous environment of retail stores. Attacks on sensitive data in memory, in transit, and at rest are not the