

Microsoft

MICROSOFT PROFESSIONAL

Threat Modeling

*Frank Swiderski
Window Snyder*

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Copyright © 2004 by Microsoft Corporation

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

Library of Congress Cataloging-in-Publication Data
Swiderski, Frank.

Threat Modeling / Frank Swiderski and Window Snyder.

p. cm.

Includes index.

ISBN 0-7356-1991-3

1. Computer security. 2. Computer networks--Security measures. I. Snyder, Window.

II. Title.

QA76.9.A25S934 2004
005.8--dc22

2004049976

Printed and bound in the United States of America.

1 2 3 4 5 6 7 8 9 QWE 9 8 7 6 5 4

Distributed in Canada by H.B. Fenn and Company Ltd.

A CIP catalogue record for this book is available from the British Library.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/learning/books/. Send comments to mspinput@microsoft.com.

Microsoft, Microsoft Press, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Robin Van Steenburgh

Project Editor: Karen Szall

Indexer: Richard Shrout

Body Part No. X10-46134

Introduction

The process of threat modeling is not new. In truth, the concept of threat modeling did not originate in any book. The threat modeling methodology presented here and elsewhere is a process that attackers, security researchers, and others tend to follow inadvertently and have followed for some time. This is the strength of the approach this book advocates: it models the thought processes of an adversary who is attempting to achieve a set of goals with respect to a defined system.

A system can be attacked only if it has *entry points*—that is, transition points between the system in question and other systems that data or commands traverse. Furthermore, an adversary will attack a system only if that system has one or more assets of value. Based on these two ideas, threat modeling seeks to enumerate the goals an adversary has when attacking a system, investigate those goals for mitigation, and remedy them. In doing so, development teams begin creating a security specification for a system.

The term *threat* denotes an adversary's goal. Other texts might use this term to describe the adversary himself. Or they might use the term to describe the capability of an adversary to attack a system. In this book, however, threats refer to goals, and the sum of all goals for a system is considered the system's *threat profile*. In addition, the term *vulnerability* denotes a set of conditions that must occur or be true for a threat to be realized. This fits quite well with using threat trees to investigate threats to a system.

More Info Chapter 2 presents a more thorough list of the key threat modeling terms used in this book.

The Threat Modeling Process

This book presents a process that is certainly more formalized than what most attackers adhere to. Attackers do not take the time to enumerate all system assets, nor do they collect all the background information this book recom-

mends. At the same time, the process could be even more formal than described in this book. The goal of this book is to describe a thought process, or methodology, that can be applied to any development environment—from the most casual to the most rigorous.

This book does not prescribe the use of Unified Modeling Language (UML) or any other formalized modeling as part of its methodology for a couple of reasons:

- Not all development environments are the same, and not all developers use or are familiar with UML. The same is true for other modeling techniques. Instead of limiting the methodology to specific technologies, this book presents a process that can be integrated into any environment.
- This methodology is intended to be customized; however, development teams need to adhere to its principles. Could development teams rewrite the process using UML? Certainly. Teams could also express the process in terms of other standards. For example, in Chapter 4, even the preferred data flow model—data flow diagrams (DFDs)—is interchangeable with other techniques.

Who Should Read This Book?

A number of members of project development teams can benefit from the methodology presented in this book:

- **Security process managers (SPMs)** The most important audience for this book is comprised of the SPMs of a development project. An SPM has the responsibility of applying the threat modeling methodology to the development environment. In addition, the SPM must drive the application security life cycle, educating other team members about the security process.
- **Program managers** These managers must “own” individual threat model documents and efforts, ensuring that they are scheduled and completed effectively for the system to benefit from them.
- **Architects and developers** Solution architects and developers will use the information in this book to guide them through the process of developing and understanding threats to the system so that they can create secure systems.

- **Software testers** Testers, who play an important role in threat modeling, provide a critical eye to analyzing the security of the system. Testers must verify or disprove the security of the system, and they participate in threat models, reviews, and penetration tests.

What Will Development Teams Gain from This Book?

This book is not intended to be a list of common threats and vulnerabilities. Rather, it describes the process of threat modeling so that development teams can apply what they have learned to creating more secure systems. Every development environment has unique properties and characteristics. Teams reading this book are encouraged to customize the threat modeling methodology to suit their particular environments.

After reading this book, members of the development team will be able to:

- Understand the adversary's view of a system and how it differs from an architect's or developer's view
- Describe the threat profile for a system by using the data flow approach
- Find weaknesses in system architecture and implementation by using investigation techniques, such as threat trees and threat model-directed code reviews
- Provide a more credible characterization of the security of a system that has been threat modeled
- Use threat modeling to verify the security of and increase the resilience of software systems

Development team members who want to skim this book for an overview should look at Chapter 2, which describes the overall threat modeling process. Chapters 3 and 5 will also be valuable to those looking for shortcuts because they describe entry points, assets, and the threat profile. Chapter 4 describes bounding the threat model discussion. The rest of the chapters, which flesh out the threat modeling process, will be most important for a project's security process manager.