

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

Threat Modeling Terminology

Before discussing the threat modeling process, certain terms should be defined. These will be explored in more detail in subsequent chapters:

- **Asset** An abstract or concrete resource that a system must protect from misuse by an adversary.
- **Attack path** A sequence of conditions in a threat tree that must be met for an attack goal (threat) to be achieved. A valid attack path (one with no mitigated conditions) is a vulnerability.
- **Condition** A single action or weakness that must be present in an attack path for a threat to be unmitigated and therefore exploitable as a vulnerability.
- **DREAD** A ranking of the risk associated with a condition or vulnerability: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability.
- **Entry point** An interface that the system has with the outside world—that is, the transition point between some functionality controlled by the system and that which is outside its control.
- **External dependency** A dependency on another system that the security of the system being modeled must abide by to prevent potential vulnerabilities.
- **External entity** A system, user, or other component that exists outside the system being modeled but can interact with that system via one or more entry points.
- **Penetration test** A test of the implementation of a system that attempts various attack paths, to either prove or disprove the mitigation of one or more threats.
- **Risk** A characterization of the danger of a vulnerability or condition.
- **Security strength** The effectiveness of the system at mitigating a threat.
- **Security weakness** An insufficient mitigation of a threat to the system, usually resulting in a vulnerability.
- **STRIDE** A classification system that describes the effect of a threat: Spoofing, Tampering, Repudiation, Denial of service, and Elevation of privilege—in other words, what an adversary will attain if the threat is exploited as a vulnerability.

- **System** A collection of functionality that can span one or more components (functional areas). A system exposes certain functionality to external entities (interactors outside of the control of the system) and must protect one or more assets.
- **Threat** The adversary's goals, or what an adversary might try to do to a system. (The collection of all threats against a system is its threat profile.) Threats to a system always exist, regardless of mitigation.
- **Threat model** A document that provides background information on a system, the system's threat profile, and an analysis of the current system against that threat profile.
- **Threat profile** A characterization of all attack goals that an adversary has for a system. A threat profile explains what the adversary might try to do with or to the system's assets. Simply put, it is a list of threats.
- **Threat tree** An analysis tool that describes the attack paths for a particular threat. A threat tree is comprised of hierarchical conditions and allows the threat's mitigation (or lack thereof) to be characterized. The root of the threat tree is the threat that it corresponds to.
- **Trust level** A characterization of an external entity, often based on how it is authenticated and what privileges it has. Trust levels can be associated with entry points. In this case, the trust level would describe the minimum trust that an external entity should have to interface with the entry point. Trust levels can also be associated with protected resources, in which case a trust level would describe the minimum trust that an external entity should have to influence the resource.
- **Use scenario** How the system is intended (or not intended) to be used.
- **Vulnerability** A security flaw in the system that represents a valid way for an adversary to realize a threat. A threat that has an unmitigated attack path from the path's leaf conditions in a threat tree to the root threat results in a vulnerability.

Purpose and Objectives

Threat modeling is, in essence, the act of creating a security design specification and later testing that design. Thus, threat modeling is integral to the development of any secure system. If performed thoroughly and to a standard methodology, threat modeling can improve the built-in security of a system as well as