Dr. Dobbs Jolt Award Finalist 2014

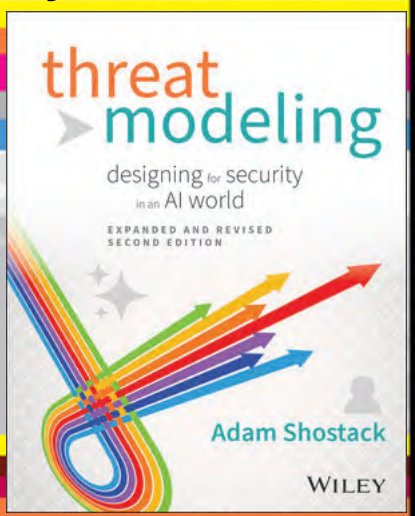
Adam Shostack
Microsoft's Threat Modeling Expert

Appendix A "Helpful Tools" from

threat modeling

designing for security

New Edition Coming January 2027



WILEY

Threat Modeling: Designing for Security

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

Published by John Wiley & Sons, Inc., Indianapolis, Indiana
Published simultaneously in Canada

ISBN: 978-1-118-80999-0
ISBN: 978-1-118-82269-2 (ebk)
ISBN: 978-1-118-81005-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Library of Congress Control Number: 2013954095

APPENDIX

A

Helpful Tools

This appendix provides you with a set of lists containing common answers to "What's your threat model?" and "What are your assets?"

Common Answers to "What's Your Threat Model?"

The question "What's your threat model?" can help you quickly express who or what you're worried about. Some typical answers include the following:

- Someone with user-level access to the machine
- Someone with admin-level access to the machine
- Someone with physical access to a machine or site

Network Attackers

Attackers that are in a good position to attack via the network include the following:

- Eve or Mallory
  - Using available software
  - Creating new software
- Your ISP

- Your cloud provider, or someone who has compromised them
- The coffee shop or hotel network
- The Mukhbarat or the NSA
- A compromised switch or router
- The node at the other end of a connection
- A trusted node that's been compromised

Physical Attackers

This section considers those physically attacking a technical system, not those attacking people. Examples include the following:

- Possession of a machine for unlimited time
  - A thief who has stolen the machine
  - Police or border agents who seize the machine
- Time-limited but physically unconstrained access
  - For five minutes
  - For an hour
  - The janitor*
  - Hotel maids*
- Physically constrained access to a machine
  - Can insert a USB key ("Can I just plug my phone in to recharge?")
  - Physical, in-line keyloggers
  - Access via Bluetooth or other radio protocols
- Ninjas
- Pirates (the kind with guns)

*Either of whom can be a techie in a uniform

There is an equivalent set of threats to the integrity and confidentiality of a network:

- Access to the network for an (effectively) unlimited time (easiest with wireless networks, including WiFi, microwave or satellite links)
- Time-limited access that allows plugging in of a "leave behind" box, such as those made by the company Pwnie Express
- Physically and temporally constrained access, such as a guest plugging into a conference room network

Attacks against People

There's a variety of ways in which people are attacked. Cryptographers are fond of talking about "rubber hose" cryptanalysis (also known as beating someone until they talk). It can be fascinating to consider what happens if each person (or class of person, such as sysadmins) in a system goes bad, but these attacks can be tremendously expensive to prevent.

For example, there is a model outlining how secret agents convince people to become spies using the following four methods (Shane, 2008):

- Money
- Ideology
- Coercion
- Ego

In this micro-model, coercion includes persuasions like rubber hose cryptanalysis, the Zapata cartel kidnapping a family member, and so on. Similarly, ego includes using sex as bait. Always remember to focus on the threats that you can mitigate.

Supply Chain Attackers

There is a set of people who can attack you through the supply chain that delivers technology to your environment. These attackers are commonly worried about, but they are hard to protect yourself against. They can attack hardware, software, and firmware, along with documentation. What's more in the era of using search engines to solve all technical problems, an attacker can augment their attacks with well-crafted untrustworthy advice on random websites in the hopes of influencing people to act in certain ways. Supply chain attackers include the following:

- System designers
  - For your system
  - For components on which you depend
- System builders
  - The factory in China building your widgets
  - A supplier to that factory who delivers parts
  - A supplier to that factory who delivers machines
- The delivery chain

Privacy Attackers

These are attackers who might violate people's privacy. They include the following:

- Marketers
  - Systems designers who rely on advertising models
  - Component libraries who sell to marketers
- Data brokers
- Stalkers
- Identity thieves
- The NSA or other national intelligence agencies
- Police
  - Constrained by laws in the way democracies expect
  - Not/less constrained by law
- Those linking databases

Non-Sentient "Attackers"

Non-sentient attackers such as the following generally don't attack the confidentiality or integrity of your systems, but they can absolutely impact its availability:

- Natural disasters (as appropriate for your region)
- Public health disasters

The Internet Threat Model

As discussed in Chapter 17, "Bringing Threat Modeling to Your Organization," the IETF has adapted a standard threat model for the design of new Internet protocols. The document is a fascinating example of how security experts can design a custom threat modeling approach for an organization. Note that revelations by Edward Snowden in late 2013 may change this model.

> *The Internet environment has a fairly well understood threat model. In general, we assume that the end-systems engaging in a protocol exchange have not themselves been compromised. Protecting against an attack when one of the end-systems has been compromised is extraordinarily difficult. It is, however, possible to design protocols which minimize the extent of the damage done under these circumstances.*

By contrast, we assume that the attacker has nearly complete control of the communications channel over which the end-systems communicate. This means that the attacker can read any PDU (Protocol Data Unit) on the network and undetectably remove, change, or inject forged packets onto the wire. This includes being able to generate packets that appear to be from a trusted machine. Thus, even if the end-system with which you wish to communicate is itself secure, the Internet environment provides no assurance that packets which claim to be from that system in fact are.

Rescorla and Korver, *Security Considerations Guidelines* (RFC 3552)

The IETF also considers two classes of limited threat models: passive attackers who will read from but not write to the network, and active attackers who can write, and possibly read.

Assets

Please only use this section after you have considered the risks and difficulties of asset-centric modeling, as discussed in Chapters 2 "Strategies for Threat Modeling" and 19 "Architecting for Success."

Computers as Assets

You can label various types of computers as assets, including the following:

- Computers used by individuals
  - This computer
  - A laptop
  - A mobile phone
  - iPad/Kindle/Nook
  - etc.
- Servers
  - Web server
  - E-mail server
  - Database server
  - etc.
- Security systems
  - Firewall
  - VPN concentrator
  - Log server

- Functional groups
  - Development systems
  - Financial systems
  - Manufacturing systems

People as Assets

You can think of people as assets who could come under attack. (Of course, it is more correct to consider them as resources.) Some groups of people you might consider include the following:

- Executives
  - Executive assistants
- Sysadmins
- Sales people
- Janitorial staff
- Food-processing staff
- Contractors of various stripes
- Any employee
- Citizens
- Immigrants
- Minorities
- People living with disabilities

Processes as Assets

You can consider your processes as assets. Examples include the following:

- Issuing a check/money transfer (including refunds)
- Shipping product (or product keys)
- Software or product development
  - Deployment
- Manufacturing
  - Integrity of product
  - Safety of workers
- Hiring

Intangible Assets

The reasoning behind including intangible assets is that because they're listed on the balance sheet, they should be listed in the threat model. However, there's a chasm between these assets and threats that you can mitigate. Regardless, here are some examples:

- Reputation or goodwill
- Intellectual property
- Stock price
- Executive attention
- Operational staff attention
- Employee morale

Stepping-Stone Assets

These are assets in the most limited sense, but they are sometimes used:

- Authentication data
  - Username/password
  - Physical access tokens
  - Mobile phones pretending to be access tokens
- Network access
- Access to a particular computer