Dr. Dobbs Jolt Award Finalist 2014

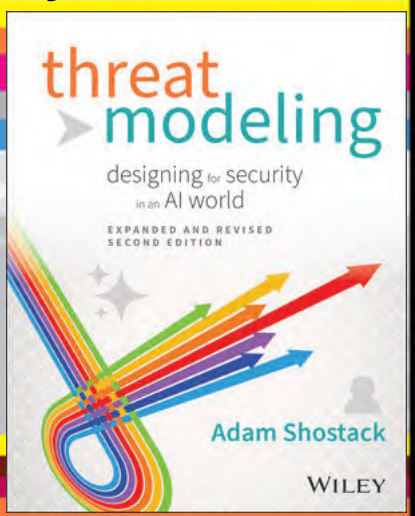
Adam Shostack
Microsoft's Threat Modeling Expert

Appendix C "Attacker Lists" 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

C

Attacker Lists

As discussed in Chapter 2, "Strategies for Threat Modeling," focusing on attackers is an attractive way to make threats real. This appendix provides you with an understanding of attackers at a variety of levels of details. The first section is four lists of attackers with limited detail about each. That is followed by a discussion of "personas," and then a fully worked out system of threat personas.

Many projects have floundered because creating these models is challenging. This appendix is presented with the hope that it will help you, and the (cynical) expectation that it will help you by helping you "fail faster." That is, by providing these lists, you can experiment with a variety of attacker models, rather than needing to create your own to try them out. By failing faster, you can learn lessons and move along, rather than getting mired in an approach.

There is one other attacker worth considering, and that is the expert witness. If you expect your product (or evidence from it) to be used in court, consider how each element of the product, process, or system might come under attack by a motivated skeptic. For an example of this, see "Offender Tagging" by Ross Anderson (Anderson, 2013).

Attacker Lists

This section lays out four sets of attackers which have been developed to various degrees.

Barnard's List

One set of attackers was developed by Robert Barnard in *Intrusion Detection Systems* (Barnard, 1988) and is covered in Ross Anderson's *Security Engineering, 2nd Edition* (Wiley, 2008, pp. 367-68). It consists of four attackers. Derek, a 19-year-old addict, is looking to steal to pay for his drugs. Charlie is a cat burglar who has been convicted seven times. Bruno is a "gentleman criminal" who steals art or other high-value items. Abdurrahman heads a cell of militants with military weapons training and technical support from a small government.

Verizon's Lists

Another set of attackers appears in the Verizon Data Breach Intelligence Report, and is derived from observation of their data. It consists of three types of actors who appear regularly: organized crime, state affiliated, and activists. Each is characterized by the industry of victims they attack, the region in which they operate, common actions, and the sorts of assets they go after. (Verizon, 2013).

NOTE **Verizon uses the word "asset" to refer to either a machine type, such as "mail server," or the data that the attackers want, or both. This is yet another example of how the term can reduce clarity, rather than add it, as discussed in Chapter 2.**

This attacker set is best suited for operational threat modeling. A slight variant of this is used by the security company Securosis, which adds "competitor," and replaces "activists" with "unsophisticated" (Securosis, 2013).

Verizon's RISK team also has what they call the "A4 Threat Model." A4 refers to Actors, Actions, Assets, and Attributes. (Verizon, 2013). Based on conversations with the creators, that model may be better for categorizing incidents than predicting them.

OWASP

The Open Web Application Security Project (OWASP) has a set of attackers in (OWASP, 2012). The OWASP enumeration of threat agents is quoted verbatim below:

- **Non-Target Specific:** Non-Target Specific Threat Agents are computer viruses, worms, trojans, and logic bombs.

- **Employees:** Staff, contractors, operational/maintenance personnel, or security guards who are annoyed with the company
- **Organized Crime and Criminals:** Criminals target information that is of value to them, such as bank accounts, credit cards, or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- **Corporations:** Corporations who are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- **Human, Unintentional:** Accidents, carelessness
- **Human, Intentional:** Insider, outsider
- **Natural:** Flood, fire, lightning, meteor, earthquakes

Intel TARA

Intel has a system called Threat Agent Risk Assessment (TARA) that includes a Threat Agent Library and a Methods and Objectives Library. The system is described in a white paper from Intel, but the complete libraries are considered confidential (Rosenquist, 2009). The Intel TAL consists of 22 threat agents, and a 16-agent derivative is included in the U.S. Department of Homeland Security's "IT Sector Baseline Risk Assessment." A list of "Threat Agent Profiles" is included in Figure 4 of the TARA paper, and it includes the following agents:

- Competitor
- Data miner
- Radical activist
- Cyber vandal
- Sensationalist
- Civil activist
- Terrorist
- Anarchist
- Irrational individual
- Government cyber warrior
- Organized criminal
- Corrupt government official
- Legal adversary
- Internal spy
- Government spy

- Thief
- Vendor
- Reckless employee
- Untrained employee
- Information partner
- Disgruntled employee

Personas and Archetypes

It's possible to start from a simple list of attacker archetypes, such as those shown in the previous section. When doing so, it's easy to find yourself arguing about the resources or capabilities of such an archetype, and needing to flesh them out. For example, what if your terrorist is state-sponsored, and has access to government labs? These questions make the attacker-centric approach start to resemble "*personas*," which are often used to help think about human interface issues. You can use lessons from that community to inform your approach.

Although he didn't invent the word, usability pioneer Alan Cooper developed the concept of personas in his 1998 book, "*The Inmates are Running the Asylum*" (SAMS, 1999). In more recent work, "*About Face 3*: *The Essentials of Interaction Design*" (Wiley, 2012), Cooper and his colleagues integrate personas into a more in-depth process, and stress that personas are based on research. Cooper defines a seven step process for creating personas.

1. Identify behavioral variables.
2. Map interview subjects to behavioral variables.
3. Identify significant behavior patterns.
4. Synthesize characteristics and relevant goals.
5. Check for completeness and redundancy.
6. Expand descriptions of attributes and behaviors.
7. Designate persona types.

They defined this process because experience with less structured approaches didn't lead to effective product design. They stress that persona development must be an intensive data- and research-driven process. If you're willing to go through that sort of process for an attacker set, then you may find more success with attacker-driven threat modeling. For step 2, you may be able to find multiple attackers of each type and induce them to go through your interviews. Then, with such a persona set in hand, you may able to create useful scenarios and requirements.

A key aspect of Cooper's approach to scenarios and requirements is that people are using a product to accomplish goals, and the reason for the personas is to ensure that features are created in support of those goals. Unless you include a "give me administrator access" button, attackers are unlikely to use the features you create in the way you intend to accomplish their goals.

With that explanation of personas, let's proceed to a fully-worked set of attacker personas.

Aucsmith's Attacker Personas

The remainder of this appendix is a reformatted and very gently edited version of a document, "Threat Personas," (Aucsmith, 2003) created between 1999 and 2003 by Dave Aucsmith, Brendan Dixon, and Robin Martin-Emerson at Microsoft, and it appears here with the kind permission of Microsoft. Note that some of the list elements were left empty in the original, and those have been left empty here.

It is included because it is a well-worked-through and empirical approach to persona-driven threat modeling. It can help you by accelerating experiments with such approaches. However, you should also see the cautions in Chapter 2, before attempting to use these personas.

Background and Definitions

All computer systems have both users and, in some sense, anti-users: those trying, for one reason or another, to break into, control, or misuse a computer system and the data it manages. Anti-users, like computer users, fall into a few patterns that describe "threat personas" engaged in "threat scenarios."

Classification of anti-users, based on an analysis of FBI cyber-attack data, clusters best when using two key axes: Motivation and Skill. There are four different motivations driving anti-users:

- **Curiosity:** "Because it was there" compels some anti-users. They want to experiment and try things out, perhaps indulging in a little vandalism along the way. They're not motivated by fame or gain (yet), but wile away the hours for their own enjoyment. A common physical analogy is kids who vandalize local parks for no apparent reason.
- **Personal fame:** Some anti-users want fame; they like to see their name "in lights" or to be known among their friends and comrades. Financial gain is not a goal. These anti-users purposely leave marks for others to see, to build their own reputation. A physical analogy might be those who block streets to protest the WTO.

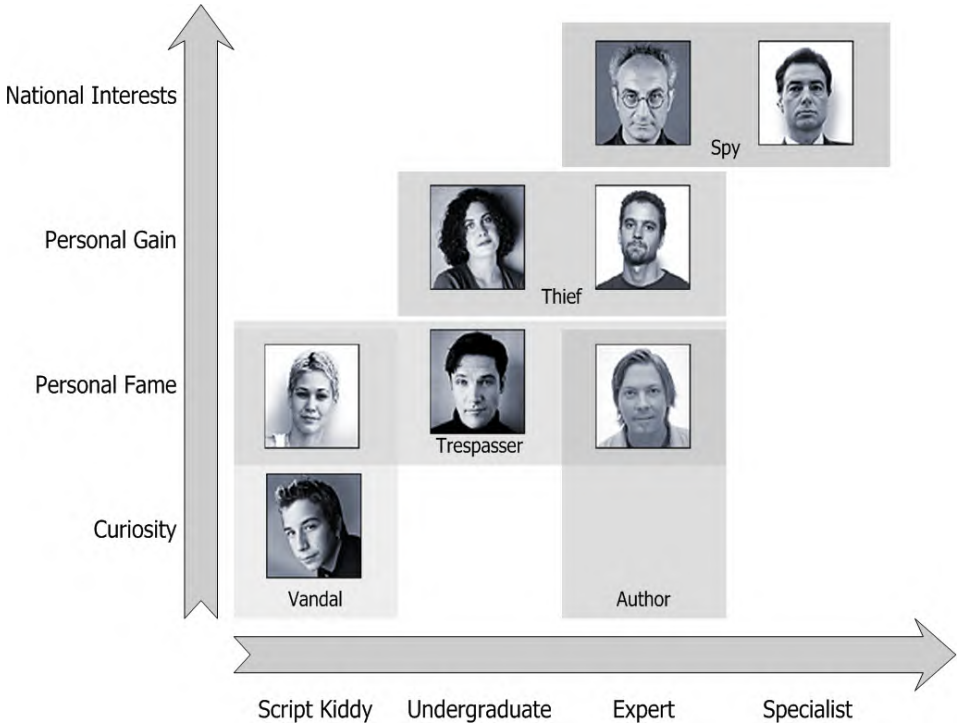
- **Personal gain:** A growing number of anti-users use their skills for personal gain. These range from spammers (who co-opt innocent systems for use as spam mailers) to those that commit financial fraud (such as by stealing credit card numbers). What sets these apart is the desire for personal financial gain. Bank robbers, in the physical world, have the same motivation.
- **National interests:** Political interests drive a select number of anti-users. To them, "hacking" is just another tool for accomplishing a political end. There are *legitimate* anti-users, such as those protecting a country's national interests, and *illegitimate* anti-users seeking to undermine that same interest. A legitimate anti-user, for example, might crack into a terrorist's computer to learn of an impending attack; an illegitimate anti-user, by contrast, may attack an airline reservation system to learn flight passenger details. The nation they serve, by standard definitions, might or might not exist (such as Al-Qaeda). Physical analogies abound and span the globe. They include the NSA (National Security Agency) in the US, the GCHQ in Britain, and other known (or unknown) organizations.

Anti-users also have varying levels of skill:

- **The script kiddie:** Because programs, once written, may be used by anyone, not all anti-users are themselves programmers. Some merely use the tools and applications others develop. These script-kiddies do not have any real system knowledge—they only understand how to follow instructions and use the different available tools.
- **The undergraduate:** A little knowledge can go a long way. A number of anti-users have bits of experience coupled with some undergraduate experience. They employ these much like the script kiddies: They mostly use tools and applications other write. They might try some minor modifications, such as tailoring the attack or slightly altering the data used, but they lack the skills to do anything more than twist and adjust a few dials and settings.
- **The expert:** Advanced anti-users supply the tools and applications. They write the worms and viruses. They write the worm generators and virus generators. They write the applications that snoop networks for weaknesses. They're quite comfortable working in the kernel of their favorite operating system or reading protocol traces. Advanced anti-users are the experts of the underground.

- **The specialist:** Virtually any skill has a value to someone, and "hacking" skills are worth a great deal to some. A few anti-users, through very specialized training (such as Ph.D. work) and access to critical resources (such as significant monetary funds and source listings), develop extremely specialized abilities. These specialists do not often leave traces of their work. They work carefully and methodically. Snooping and breaking computer systems is their job, not just their pastime.

When applied to the FBI data, these motivation and skill categories yield eight, distinct threat personas grouped by five different "behaviors"—a two-way interaction between motivation and skill—as depicted in the following figure. The following sections cover each persona in detail.



Personas

David "Ne0phyate" Bradley – Vandal

Overview

MOTIVATION	❖ Curiosity ❖ Experimentation
SKILL AND EDUCATION	❖ Quintessential script kiddie ❖ Freshman in computer science
SPAN OF INFLUENCE	❖ None
COLLABORATION	❖ Depends on "publicly" available tools and applications ❖ Does not contribute to others; is a "lurker"
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	❖ None

Core Profile

Chief Motivation

- Curiosity

Background, Experience, and Education

- Most common type of attacker; frequently participates in DDoS attacks
- Has played with computers for years; is the computer "expert" for his family and friends
- Frequently plays computer games
- Very little programming experience, restricted to scripting websites
- Has "no clue" regarding details of the attacks he launches, but he is persistent and has the time. He'll try anything without regard for the consequences (e.g., run attacks meant for Windows against Linux systems).
- Never attacks early in the morning (because he's sleeping); attacks most always occur late in the evening or on weekends
- Currently a freshman in computer science

Employer

- None, is a full-time student

Previous Accomplishments

- Launched a three-day TCP/IP "SYN flood" DoS attack against a non-profit organization; also tried using an ICMP "ping-of-death" attack (which failed)
- Recently knocked all friends off of an IRC (Internet Relay Chat) session using a DoS (Denial of Service) script
- Unsuccessfully attempted to gain administrator (aka "root") access to the Department of Computer Science lab computers
- Took part in two of the large DDoS attacks launched against well-known sites (e.g., Yahoo!)
- More or less attended class during the last week

Span of Influence

- None, depends highly on others

Scope of Attacks

- Popular websites
- His school's network

- Friends' computers
- Computers on his cable modem network segment (e.g., his neighbors)

JoLynn "NightLily" Dobney – Trespasser

Overview

MOTIVATION	❖ Personal fame; bragging rights ❖ Experimentation
SKILL AND EDUCATION	❖ Basic programming and network knowledge ❖ Self-taught ❖ Heavily reads news groups
SPAN OF INFLUENCE	❖ None
COLLABORATION	❖ Depends on "publicly" available tools and applications ❖ Does not contribute to others; is a "lurker"
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	❖ Limited; typical low-level system jockey

Core Profile

Chief Motivation

- Personal fame

Background, Experience, and Education

- Has played with computers for years; is the computer "expert" for her family and friends
- Frequently plays computer games
- Has a little more knowledge and experience than script kiddies, but not much more—likes to experiment, though, and try new things
- Some programming experience; can write some system scripts and configure standard components (e.g., network router)
- Mostly self-taught; possible computer tech degree

Employer

- Computer technician in a medium-size manufacturing plant

Previous Accomplishments

- Periodically shuts down local library website through IRC-based DDoS (distributed denial-of-service) attacks
- Nightly runs scripts to find open computers on cable modem network segment
- Planted a Sub7 Trojan horse program (a "backdoor" allowing continued access to the computer) on open computers
- Attacked her local community library, with persistent DoS attacks, to contest a $0.25 late-return fine
- Unintentionally destroyed data used by a medium-size website when the Trojan horse she implanted caused the web server to fault

Span of Influence

- None, depends highly on others

Scope of Attacks

-

Sean "Keech" Purcell – Defacer

Overview

MOTIVATION	❖ Seeks to change public opinion; vent personal anger ❖ Conscience; morally-motivated political goals ❖ Personal fame
SKILL AND EDUCATION	❖ Enrolled in an MS in computer science program ❖ Attends Black Hat ("hacker" convention)
SPAN OF INFLUENCE	
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	

Core Profile

Chief Motivation

- Political purposes

Background, Experience, and Education

- Moderate programming and network experience, mostly in applications
- Completed an undergraduate in computer science
- Enrolled in an MS in computer science program
- Relatively sophisticated and reasonably skilled (He doesn't write the original exploit but he can cobble together new combinations and modify how the exploit works.)
- Active member of the "Animal Liberation Front" (ALF) that recently released 10,000 minks from "captivity" on a local mink farm
- Differs from a terrorist only by a matter of degree; he has the same essential motivation and uses similar (though less sophisticated) methods

Employer

- Currently a full-time student

Previous Accomplishments

- Recently changed the FRAMESET URLs of a wood products company's home page; he left the company's name intact but replaced the content with a political diatribe against their tree harvesting techniques
- Changed the home page of a wood products company, by exploiting an IIS vulnerability, to point to the home page of an environmental advocacy group
- Successfully launched a DDoS attack against the same wood products company

Span of Influence

-

Scope of Attacks

-

Bryan "CrossFyre" Walton – Author

Overview

MOTIVATION	❖ Personal fame among his small circle of "authors"
SKILL AND EDUCATION	❖ Holds an MS in computer science
SPAN OF INFLUENCE	
COLLABORATION	❖ Contributes "public" tools for others to use
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	

Core Profile

Chief Motivation

- Personal fame among fellow "authors"

Background, Experience, and Education

- Has played with computers for years; is the computer "expert" for his family and friends

- Extensive programming and network experience, both in applications and systems
- Holds an MS in computer science
- Reads and contributes to news groups; seen as one of the "experts"
- Is hard to track down and little concrete information is known about him; what is known has been learned by rumor and innuendo.
- He writes the exploit, perhaps just the kernel of the attack; he lets others (using toolkits) build and launch the actual worm or virus.
- Often learns about holes by examining the patches and fixes we ship (e.g., he compares the code before and after applying the patch)

Employer

- A medium-size network management company

Previous Accomplishments

- Wrote and launched *Slammer* (a very sophisticated worm); it was unusual that he elected to write and launch the worm himself.
- Wrote the core of the MSBlaster worm; others packaged his exploit and launched the worm.
- Wrote a few less successful exploits against IIS and Apache
- Wrote a series of time-limited worms to test propagation techniques
- Recently contributed a new worm tool that makes it easy to launch the same worm against different operating systems

Span of Influence

- Highly influential

Scope of Attacks

-

Lorrin Smith-Bates – Insider

Overview

MOTIVATION	❖ Personal gain ❖ Intense dislike for her employer
SKILL AND EDUCATION	❖ Holds a BS in computer science ❖ Three years of experience as a database administrator
SPAN OF INFLUENCE	❖ Very limited ❖ Does not actively participate in the underground community
COLLABORATION	❖ None
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	❖ Three years of experience as a database administrator ❖ Held two summer internships while completing her undergraduate degree (one as a phone-support technician, another as a network jockey)

Core Profile

Chief Motivation

- Personal gain

Background, Experience, and Education

- Regularly uses computers but is not avid user (e.g., not a frequent gamer)
- Some programming experience; mostly application level, some systems level
- Has held internships as a phone-support technician and as a network jockey
- Has been employed for the last three years as a database administrator for the accounting database; highly trusted by the organization, usually has access to bookkeeping functions and/or systems

Employer

- Medium-size retail firm

Previous Accomplishments

- Recently modified the access permissions on the purchasing database. Set herself up as a vendor and billed the company for consumables; was caught when the discrepancy was detected during an in-depth audit
- In her previous job, with a large NY bank, she initiated a false interbank transfer (SWIFT) into an accomplice's London account.

Span of Influence

- Very limited
- Does not actively participate in the underground community

Scope of Attacks

- Limited to her current employer

Douglas Hite – Thief

Overview

MOTIVATION	❖ Personal gain ❖ The thrill of succeeding
SKILL AND EDUCATION	❖ Holds a BS in computer science ❖ Has eight (or more) years of system-level programming experience
SPAN OF INFLUENCE	
COLLABORATION	
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	❖ Systems-level programmer for several years

Core Profile

Chief Motivation

- Personal gain

Background, Experience, and Education

- Has played with computers for years; is the computer "expert" for his family and friends

- Frequently plays computer games
- A great deal of programming experience, in both applications and especially systems
- Holds a BS in computer science
- Has eight (or more) years of system-level programming experience writing drivers for remote-control devices
- He is, effectively, a member of organized crime moving into the computer world; the fastest growing segment of computer crime (e.g., the Russian Mafia is getting very good at this).

Employer

- Crime-based organization
- May hold a day job?

Previous Accomplishments

- Obtained credit-card numbers from CDNow via a 24-byte SQL injection attack. He then offered goods on eBay, which, when purchased, he bought using one of the stolen numbers (pocketing the auction price and leaving the victim with "hot" goods).
- Attacked a medium-size doctor's office just before payday, redirecting all direct-deposit information to his own account(s). Then, after payday, he redirected the direct-deposit information back to the correct entries, covering his tracks.
- Modified DNS entries for a ticket agency's computers. This redirected a FORM POST to purchase tickets to a false clearinghouse. He collected the real tickets and cashed them in for face value at different airports.

Span of Influence

-

Scope of Attacks

-

Mr. Smith – Terrorist

Overview

MOTIVATION	❖ National interests ❖ Highly motivated by ideology
SKILL AND EDUCATION	❖ Holds an MS in computer science ❖ Seven (or more) years experience in systems-level programming
SPAN OF INFLUENCE	❖ Limited to his ideological organization ❖ Quiet and does seek to influence "outsiders"
COLLABORATION	❖ Member of an ideological organization ❖ Works with assigned "team" members
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	❖ Several years of experience as a systems-level programmer

Core Profile

Chief Motivation

- National interests (motivated by ideology)

Background, Experience, and Education

- Holds an MS in computer science
- Seven (or more) years experience in systems-level programming
- Trained in weapons and explosives
- Deeply committed to the ideological principles of his organization

Employer

-

Previous Accomplishments

- Hacked into a Kuwaiti airline reservation system and found flights carrying members of the Kuwaiti royal family. He relayed this information to a compatriot who then blew up the plane in flight.
- Stole information on aerosol physics to assist with manufacturing chemical weapons
- Located a truck shipment of organophosphates (used to make nerve gas) in England. He then assisted with hijacking the truck.

Span of Influence

- Limited to his ideological organization
- Quiet and does seek to influence "outsiders"

Scope of Attacks

- Worldwide

Mr. Jones – Spy

Overview

MOTIVATION	❖ National interests
SKILL AND EDUCATION	❖ Holds a Ph.D. in computer science ❖ Continuous and ongoing education and training
SPAN OF INFLUENCE	
COLLABORATION	
TOOLS AND TECHNOLOGIES	
IT EXPERIENCE	

Core Profile

Chief Motivation

- National interests

Background, Experience, and Education

- Holds a Ph.D. in computer science (His thesis was "Fault Injection into Cryptographic Protocols.")
- Actively engaged in continuous education and training
- Has access to most source code (legally or illegally obtained)

Employer

- Government agency

Previous Accomplishments

- By bridging through a dual-homed (two network cards) laptop, he simultaneously connected to both the Internet and a VPN. He then "echoed" every packet sent or received, using modified network drivers, to a secure collection point.
- Modified the random number generator in an OEM software image by reducing the complexity of the LFSR and then encrypting the output with a public key.

Span of Influence

-

Scope of Attacks

- Worldwide