

Contents

Introduction	xxi
Part I Getting Started	1
Chapter 1 Dive In and Threat Model!	3
Learning to Threat Model	4
What Are You Building?	5
What Can Go Wrong?	7
Addressing Each Threat	12
Checking Your Work	24
Threat Modeling on Your Own	26
Checklists for Diving In and Threat Modeling	27
Summary	28
Chapter 2 Strategies for Threat Modeling	29
“ <i>What’s Your Threat Model?</i> ”	30
Brainstorming Your Threats	31
Brainstorming Variants	32
Literature Review	33
Perspective on Brainstorming	34
Structured Approaches to Threat Modeling	34
Focusing on Assets	36
Focusing on Attackers	40
Focusing on Software	41
Models of Software	43
Types of Diagrams	44
Trust Boundaries	50
What to Include in a Diagram	52
Complex Diagrams	52
Labels in Diagrams	53

	Color in Diagrams	53
	Entry Points	53
	Validating Diagrams	54
	Summary	56
Part II	Finding Threats	59
Chapter 3	STRIDE	61
	Understanding STRIDE and Why It's Useful	62
	Spoofing Threats	64
	Spoofing a Process or File on the Same Machine	65
	Spoofing a Machine	66
	Spoofing a Person	66
	Tampering Threats	67
	Tampering with a File	68
	Tampering with Memory	68
	Tampering with a Network	68
	Repudiation Threats	68
	Attacking the Logs	69
	Repudiating an Action	70
	Information Disclosure Threats	70
	Information Disclosure from a Process	71
	Information Disclosure from a Data Store	71
	Information Disclosure from a Data Flow	72
	Denial-of-Service Threats	72
	Elevation of Privilege Threats	73
	Elevate Privileges by Corrupting a Process	74
	Elevate Privileges through Authorization Failures	74
	Extended Example: STRIDE Threats against Acme-DB	74
	STRIDE Variants	78
	STRIDE-per-Element	78
	STRIDE-per-Interaction	80
	DESIST	85
	Exit Criteria	85
	Summary	85
Chapter 4	Attack Trees	87
	Working with Attack Trees	87
	Using Attack Trees to Find Threats	88
	Creating New Attack Trees	88
	Representing a Tree	91
	Human-Viewable Representations	91
	Structured Representations	94
	Example Attack Tree	94
	Real Attack Trees	96
	Fraud Attack Tree	96
	Election Operations Assessment Threat Trees	96
	Mind Maps	98

	Perspective on Attack Trees	98
	Summary	100
Chapter 5	Attack Libraries	101
	Properties of Attack Libraries	101
	Libraries and Checklists	103
	Libraries and Literature Reviews	103
	CAPEC	104
	Exit Criteria	106
	Perspective on CAPEC	106
	OWASP Top Ten	108
	Summary	108
Chapter 6	Privacy Tools	111
	Solove's Taxonomy of Privacy	112
	Privacy Considerations for	
	Internet Protocols	114
	Privacy Impact Assessments (PIA)	114
	The Nymity Slider and the Privacy Ratchet	115
	Contextual Integrity	117
	Contextual Integrity Decision Heuristic	118
	Augmented Contextual Integrity Heuristic	119
	Perspective on Contextual Integrity	119
	LINDDUN	120
	Summary	121
Part III	Managing and Addressing Threats	123
Chapter 7	Processing and Managing Threats	125
	Starting the Threat Modeling Project	126
	When to Threat Model	126
	What to Start and (Plan to) End With	128
	Where to Start	128
	Digging Deeper into Mitigations	130
	The Order of Mitigation	131
	Playing Chess	131
	Prioritizing	132
	Running from the Bear	132
	Tracking with Tables and Lists	133
	Tracking Threats	133
	Making Assumptions	135
	External Security Notes	136
	Scenario-Specific Elements of	
	Threat Modeling	138
	Customer/Vendor Trust Boundary	139
	New Technologies	139
	Threat Modeling an API	141
	Summary	143

Chapter 8	Defensive Tactics and Technologies	145
	Tactics and Technologies for Mitigating Threats	145
	Authentication: Mitigating Spoofing	146
	Integrity: Mitigating Tampering	148
	Non-Repudiation: Mitigating Repudiation	150
	Confidentiality: Mitigating Information Disclosure	153
	Availability: Mitigating Denial of Service	155
	Authorization: Mitigating Elevation of Privilege	157
	Tactic and Technology Traps	159
	Addressing Threats with Patterns	159
	Standard Deployments	160
	Addressing CAPEC Threats	160
	Mitigating Privacy Threats	160
	Minimization	160
	Cryptography	161
	Compliance and Policy	164
	Summary	164
Chapter 9	Trade-Offs When Addressing Threats	167
	Classic Strategies for Risk Management	168
	Avoiding Risks	168
	Addressing Risks	168
	Accepting Risks	169
	Transferring Risks	169
	Ignoring Risks	169
	Selecting Mitigations for Risk Management	170
	Changing the Design	170
	Applying Standard Mitigation Technologies	174
	Designing a Custom Mitigation	176
	Fuzzing Is Not a Mitigation	177
	Threat-Specific Prioritization Approaches	178
	Simple Approaches	178
	Threat-Ranking with a Bug Bar	180
	Cost Estimation Approaches	181
	Mitigation via Risk Acceptance	184
	Mitigation via Business Acceptance	184
	Mitigation via User Acceptance	185
	Arms Races in Mitigation Strategies	185
	Summary	186
Chapter 10	Validating That Threats Are Addressed	189
	Testing Threat Mitigations	190
	Test Process Integration	190
	How to Test a Mitigation	191
	Penetration Testing	191

	Checking Code You Acquire	192
	Constructing a Software Model	193
	Using the Software Model	194
	QA'ing Threat Modeling	195
	Model/Reality Conformance	195
	Task and Process Completion	196
	Bug Checking	196
	Process Aspects of Addressing Threats	197
	Threat Modeling Empowers Testing;	
	Testing Empowers Threat Modeling	197
	Validation/Transformation	197
	Document Assumptions as You Go	198
	Tables and Lists	198
	Summary	202
Chapter 11	Threat Modeling Tools	203
	Generally Useful Tools	204
	Whiteboards	204
	Office Suites	204
	Bug-Tracking Systems	204
	Open-Source Tools	206
	TRIKE	206
	SeaMonster	206
	Elevation of Privilege	206
	Commercial Tools	208
	ThreatModeler	208
	Corporate Threat Modeller	208
	SecurITree	209
	Little-JIL	209
	Microsoft's SDL Threat Modeling Tool	209
	Tools That Don't Exist Yet	213
	Summary	213
Part IV	Threat Modeling in Technologies and Tricky Areas	215
Chapter 12	Requirements Cookbook	217
	Why a "Cookbook"?	218
	The Interplay of Requirements, Threats,	
	and Mitigations	219
	Business Requirements	220
	Outshining the Competition	220
	Industry Requirements	220
	Scenario-Driven Requirements	221
	Prevent/Detect/Respond as a Frame	
	for Requirements	221
	Prevention	221
	Detection	225

Response	225
People/Process/Technology as a Frame	
for Requirements	227
People	227
Process	228
Technology	228
Development Requirements vs. Acquisition Requirements	228
Compliance-Driven Requirements	229
Cloud Security Alliance	229
NIST Publication 200	230
PCI-DSS	231
Privacy Requirements	231
Fair Information Practices	232
Privacy by Design	232
The Seven Laws of Identity	233
Microsoft Privacy Standards for Development	234
The STRIDE Requirements	234
Authentication	235
Integrity	236
Non-Repudiation	237
Confidentiality	238
Availability	238
Authorization	239
Non-Requirements	240
Operational Non-Requirements	240
Warnings and Prompts	241
Microsoft's "10 Immutable Laws"	241
Summary	242
Chapter 13 Web and Cloud Threats	243
Web Threats	243
Website Threats	244
Web Browser and Plugin Threats	244
Cloud Tenant Threats	246
Insider Threats	246
Co-Tenant Threats	247
Threats to Compliance	247
Legal Threats	248
Threats to Forensic Response	248
Miscellaneous Threats	248
Cloud Provider Threats	249
Threats Directly from Tenants	249
Threats Caused by Tenant Behavior	250
Mobile Threats	250
Summary	251

Chapter 14	Accounts and Identity	253
	Account Life Cycles	254
	Account Creation	254
	Account Maintenance	257
	Account Termination	258
	Account Life-Cycle Checklist	258
	Authentication	259
	Login	260
	Login Failures	262
	Threats to “What You Have”	263
	Threats to “What You Are”	264
	Threats to “What You Know”	267
	Authentication Checklist	271
	Account Recovery	271
	Time and Account Recovery	272
	E-mail for Account Recovery	273
	Knowledge-Based Authentication	274
	Social Authentication	278
	Attacker-Driven Analysis of Account Recovery	280
	Multi-Channel Authentication	281
	Account Recovery Checklist	281
	Names, IDs, and SSNs	282
	Names	282
	Identity Documents	285
	Social Security Numbers and Other National Identity Numbers	286
	Identity Theft	289
	Names, IDs, and SSNs Checklist	290
	Summary	290
Chapter 15	Human Factors and Usability	293
	Models of People	294
	Applying Behaviorist Models of People	295
	Cognitive Science Models of People	297
	Heuristic Models of People	302
	Models of Software Scenarios	304
	Modeling the Software	304
	Diagramming for Modeling the Software	307
	Modeling Electronic Social Engineering Attacks	309
	Threat Elicitation Techniques	311
	Brainstorming	311
	The Ceremony Approach to Threat Modeling	311
	Ceremony Analysis Heuristics	312
	Integrating Usability into the Four-Stage Framework	315

Tools and Techniques for Addressing Human Factors	316
Myths That Inhibit Human Factors Work	317
Design Patterns for Good Decisions	317
Design Patterns for a Kind Learning Environment	320
User Interface Tools and Techniques	322
Configuration	322
Explicit Warnings	323
Patterns That Grab Attention	325
Testing for Human Factors	327
Benign and Malicious Scenarios	328
Ecological Validity	328
Perspective on Usability and Ceremonies	329
Summary	331
Chapter 16 Threats to Cryptosystems	333
Cryptographic Primitives	334
Basic Primitives	334
Privacy Primitives	339
Modern Cryptographic Primitives	339
Classic Threat Actors	341
Attacks against Cryptosystems	342
Building with Crypto	346
Making Choices	346
Preparing for Upgrades	346
Key Management	346
Authenticating before Decrypting	348
Things to Remember about Crypto	348
Use a Cryptosystem Designed by Professionals	348
Use Cryptographic Code Built and Tested by Professionals	348
Cryptography Is Not Magic Security Dust	349
Assume It Will All Become Public	349
You Still Need to Manage Keys	349
Secret Systems: Kerckhoffs and His Principles	349
Summary	351
Part V Taking It to the Next Level	353
Chapter 17 Bringing Threat Modeling to Your Organization	355
How To Introduce Threat Modeling	356
Convincing Individual Contributors	357
Convincing Management	358
Who Does What?	359
Threat Modeling and Project Management	359

Prerequisites	360
Deliverables	360
Individual Roles and Responsibilities	362
Group Interaction	363
Diversity in Threat Modeling Teams	367
Threat Modeling within a Development Life Cycle	367
Development Process Issues	368
Organizational Issues	373
Customizing a Process for Your Organization	378
Overcoming Objections to Threat Modeling	379
Resource Objections	379
Value Objections	380
Objections to the Plan	381
Summary	383
Chapter 18 Experimental Approaches	385
Looking in the Seams	386
Operational Threat Models	387
FlipIT	388
Kill Chains	388
The “Broad Street” Taxonomy	392
Adversarial Machine Learning	398
Threat Modeling a Business	399
Threats to Threat Modeling Approaches	400
Dangerous Deliverables	400
Enumerate All Assumptions	400
Dangerous Approaches	402
How to Experiment	404
Define a Problem	404
Find Aspects to Measure and Measure Them	404
Study Your Results	405
Summary	405
Chapter 19 Architecting for Success	407
Understanding Flow	407
Flow and Threat Modeling	409
Stymieing People	411
Beware of Cognitive Load	411
Avoid Creator Blindness	412
Assets and Attackers	412
Knowing the Participants	413
Boundary Objects	414
The Best Is the Enemy of the Good	415
Closing Perspectives	416
“The Threat Model Has Changed”	417

On Artistry	418
Summary	419
Now Threat Model	420
Appendix A Helpful Tools	421
Common Answers to “What’s Your Threat Model?”	421
Network Attackers	421
Physical Attackers	422
Attacks against People	423
Supply Chain Attackers	423
Privacy Attackers	424
Non-Sentient “Attackers”	424
The Internet Threat Model	424
Assets	425
Computers as Assets	425
People as Assets	426
Processes as Assets	426
Intangible Assets	427
Stepping-Stone Assets	427
Appendix B Threat Trees	429
STRIDE Threat Trees	430
Spoofing an External Entity (Client/ Person/Account)	432
Spoofing a Process	438
Spoofing of a Data Flow	439
Tampering with a Process	442
Tampering with a Data Flow	444
Tampering with a Data Store	446
Repudiation against a Process (or by an External Entity)	450
Repudiation, Data Store	452
Information Disclosure from a Process	454
Information Disclosure from a Data Flow	456
Information Disclosure from a Data Store	459
Denial of Service against a Process	462
Denial of Service against a Data Flow	463
Denial of Service against a Data Store	466
Elevation of Privilege against a Process	468
Other Threat Trees	470
Running Code	471
Attack via a “Social” Program	474
Attack with Tricky Filenames	476
Appendix C Attacker Lists	477
Attacker Lists	478
Barnard’s List	478
Verizon’s Lists	478
OWASP	478
Intel TARA	479

Personas and Archetypes	480
Aucsmith’s Attacker Personas	481
Background and Definitions	481
Personas	484
<i>David “NeOphyate” Bradley – Vandal</i>	484
<i>JoLynn “NightLily” Dobney – Trespasser</i>	486
<i>Sean “Keech” Purcell – Defacer</i>	488
<i>Bryan “CrossFyre” Walton – Author</i>	490
<i>Lorrin Smith-Bates – Insider</i>	492
<i>Douglas Hite – Thief</i>	494
<i>Mr. Smith – Terrorist</i>	496
<i>Mr. Jones – Spy</i>	498
Appendix D Elevation of Privilege: The Cards	501
Spoofing	501
Tampering	503
Repudiation	504
Information Disclosure	506
Denial of Service	507
Elevation of Privilege (EoP)	508
Appendix E Case Studies	511
The Acme Database	512
Security Requirements	512
Software Model	512
Threats and Mitigations	513
Acme’s Operational Network	519
Security Requirements	519
Operational Network	520
Threats to the Network	521
Phones and One-Time Token Authenticators	525
The Scenario	526
The Threats	527
Possible Redesigns	528
Sample for You to Model	528
Background	529
The iNTegrity Data Flow Diagrams	530
Exercises	531
Glossary	533
Bibliography	543
Index	567