

Contents

Preface	xiii
Emmanuel PROUFF, Guénaél RENAULT, Matthieu RIVAIN and Colin O'FLYNN	
Part 1. Software Side-Channel Attacks	1
Chapter 1. Timing Attacks	3
Daniel PAGE	
1.1. Foundations	3
1.1.1. Execution latency in theory	4
1.1.2. Execution latency in practice	5
1.1.3. Attacks that exploit data-dependent execution latency	6
1.2. Example attacks	10
1.2.1. Example 1.1: an explanatory attack on password validation	10
1.2.2. Example 1.2: an attack on <code>xtime</code> -based AES	12
1.2.3. Example 1.3: an attack on Montgomery-based RSA	14
1.2.4. Example 1.4: a padding oracle attack on AES-CBC	17
1.3. Example mitigations	20
1.4. Notes and further references	21
1.5. References	24
Chapter 2. Microarchitectural Attacks	31
Yuval YAROM	
2.1. Background	31
2.1.1. Memory caches	31
2.1.2. Cache hierarchies	32
2.1.3. Out-of-order execution	33
2.1.4. Branch prediction	34
2.1.5. Other caches	34

2.2. The Prime+Probe attack	34
2.2.1. Prime+Probe on the L1 data cache	35
2.2.2. Attacking T-table AES	36
2.2.3. Prime+probe on the LLC	38
2.2.4. Variants of Prime+Probe	39
2.3. The Flush+Reload attack	41
2.3.1. Attack technique	41
2.3.2. Attacking square-and-multiply exponentiation	42
2.3.3. Attack variants	43
2.3.4. Performance degradation attacks	44
2.4. Attacking other microarchitectural components	45
2.4.1. Instruction cache	45
2.4.2. Branch prediction	46
2.5. Constant-time programming	47
2.5.1. Constant-time select	47
2.5.2. Eliminating secret-dependent branches	48
2.5.3. Eliminating secret-dependent memory access	49
2.6. Covert channels	50
2.7. Transient-execution attacks	51
2.7.1. The Spectre attack	51
2.7.2. Meltdown-type attacks	53
2.8. Summary	54
2.9. Notes and further references	54
2.10. References	57
Part 2. Hardware Side-Channel Attacks	65
Chapter 3. Leakage and Attack Tools	67
Davide BELLIZIA and Adrian THILLARD	
3.1. Introduction	67
3.2. Data-dependent physical emissions	67
3.2.1. Dynamic power	68
3.2.2. Static power	70
3.2.3. Electro-magnetic emissions	72
3.2.4. Other sources of physical leakages	73
3.3. Measuring a side-channel	75
3.3.1. Power analysis setup	75
3.3.2. Probes and probing methodologies	75
3.4. Leakage modeling	78
3.4.1. Mathematical modeling	78
3.4.2. Signal-to-noise ratio	81
3.4.3. Open source boards	83
3.4.4. Open source libraries for attacks	85

3.5. Notes and further references	86
3.6. References	87
Chapter 4. Supervised Attacks	91
Eleonora CAGLI and Loïc MASURE	
4.1. General framework	91
4.1.1. The profiling ability: a powerful threat model	91
4.1.2. Maximum likelihood distinguisher	94
4.2. Building a model	98
4.2.1. Generative model via Gaussian templates	98
4.2.2. Discriminative model via logistic regression	100
4.2.3. From logistic regression to neural networks	102
4.3. Controlling the dimensionality	105
4.3.1. Points of interest selection with signal-to-noise ratio	106
4.3.2. Fisher’s linear discriminant analysis	107
4.4. Building de-synchronization-resistant models	108
4.5. Summary of the chapter	112
4.6. Notes and further references	113
4.7. References	115
Chapter 5. Unsupervised Attacks	117
Cécile DUMAS	
5.1. Introduction	117
5.1.1. Supervised attacks	117
5.1.2. Unsupervised attacks	118
5.1.3. How to attack without profiling?	120
5.2. Distinguishers	122
5.3. Likelihood distinguisher	123
5.3.1. Distinguisher definition	123
5.3.2. Determining Gaussian model parameters	125
5.3.3. Linear leakage model for sensitive data	125
5.3.4. Linear leakage model for sensitive data bits	127
5.3.5. Conclusion	128
5.4. Mutual information	129
5.4.1. Information theory	129
5.4.2. Distinguisher	131
5.4.3. Bijectivity	132
5.4.4. Probability calculation	133
5.4.5. Conclusion	135
5.5. Correlation	136
5.5.1. Linear relationship – CPA	136
5.5.2. Equivalence	138
5.5.3. Conclusion	139

5.6. A priori knowledge synthesis	139
5.7. Conclusion on statistical tools	142
5.8. Exercise solutions	144
5.9. Notes and further references	149
5.10. References	150
Chapter 6. Quantities to Judge Side Channel Resilience	153
Elisabeth OSWALD	
6.1. Introduction	153
6.1.1. Assumptions and attack categories	154
6.1.2. Attack success	155
6.2. Metrics for comparing the effectiveness of specific attack vectors	156
6.2.1. Magnitude of scores	157
6.2.2. Number of needed leakage traces/success rate estimation	157
6.3. Metrics for evaluating the leakage (somewhat) independent of a specific attack vector	158
6.3.1. Signal to noise ratio	158
6.3.2. Mutual information	159
6.4. Metrics for evaluating the remaining effort of an adversary	160
6.4.1. Key rank	160
6.4.2. Average key rank measures	161
6.4.3. Relationship with enumeration capabilities	162
6.5. Leakage detection as a radical alternative to attack driven evaluations	162
6.6. Formal evaluation schemes	164
6.6.1. CC evaluations	165
6.6.2. FIPS 140-3	166
6.6.3. Worst-case adversaries	167
6.7. References	167
Chapter 7. Countermeasures and Advanced Attacks	171
Brice COLOMBIER and Vincent GROSSO	
7.1. Introduction	171
7.2. Misalignment of traces	173
7.2.1. Countermeasures	174
7.2.2. Attacks	179
7.3. Masking	180
7.3.1. Countermeasures	181
7.3.2. Attacks	182
7.4. Combination of countermeasures	183
7.5. To go further	184
7.6. References	185

Chapter 8. Mode-Level Side-Channel Countermeasures	187
Olivier PEREIRA, Thomas PETERS and François-Xavier STANDAERT	
8.1. Introduction	187
8.2. Building blocks	188
8.3. Security definitions	190
8.3.1. Authenticated encryption and leakage	191
8.3.2. Integrity with leakage	192
8.3.3. Confidentiality with leakage	193
8.3.4. Discussion	195
8.4. Leakage models	197
8.4.1. Models for integrity	198
8.4.2. Models for confidentiality	199
8.4.3. Practical guidelines	201
8.5. Constructions	201
8.5.1. A leakage-resilient MAC	201
8.5.2. A leakage-resistant encryption scheme	204
8.5.3. A leakage-resistant AE scheme	207
8.6. Acknowledgments	208
8.7. Notes and further references	208
8.8. References	210
Part 3. Fault Injection Attacks	213
Chapter 9. An Introduction to Fault Injection Attacks	215
Jean-Max DUTERTRE and Jessy CLÉDIÈRE	
9.1. Fault injection attacks, disturbance of electronic components	216
9.1.1. History of integrated circuit disturbance	216
9.1.2. Fault injection mechanisms	219
9.1.3. Fault injection benches	245
9.1.4. Fault models and fault injection simulation	253
9.2. Practical examples of fault injection attacks	262
9.2.1. Introduction	262
9.2.2. 1997 light attack on a secure product when loading a DES key	263
9.2.3. Experimental examples of an attack on a PIN identification routine	265
9.3. Notes and further references	272
9.4. References	273
Chapter 10. Fault Attacks on Symmetric Cryptography	277
Debdeep MUKHOPADHYAY and Sayandeep SAHA	
10.1. Introduction	277
10.2. Differential fault analysis	278

10.2.1. Block ciphers and fault models	278
10.2.2. DFA on AES: single-byte fault	281
10.2.3. DFA on AES: multiple-byte fault	284
10.2.4. DFA on AES: other rounds	285
10.2.5. DFA on AES: key schedule	285
10.2.6. DFA on other ciphers: general idea	286
10.3. Automation of DFA	286
10.3.1. ExpFault	287
10.4. DFA countermeasures: general idea and taxonomy	289
10.4.1. Detection countermeasures	290
10.4.2. Infective countermeasures	291
10.4.3. Instruction-level countermeasures	292
10.5. Advanced FA	292
10.5.1. Biased fault model	293
10.5.2. Statistical fault attack	293
10.5.3. Statistical ineffective fault attack	294
10.5.4. Fault template attacks	296
10.5.5. Persistent fault attacks	301
10.6. Leakage assessment in fault attacks	302
10.7. Chapter summary	305
10.8. Notes and further references	306
10.9. References	307
Chapter 11. Fault Attacks on Public-key Cryptographic Algorithms	311
Michael TUNSTALL and Guillaume BARBU	
11.1. Introduction	311
11.2. Preliminaries	312
11.2.1. RSA	312
11.2.2. Elliptic curve cryptography	314
11.3. Attacking the RSA using the Chinese remainder theorem	315
11.4. Attacking a modular exponentiation	316
11.5. Attacking the ECDSA	318
11.6. Other attack strategies	319
11.6.1. Safe errors	319
11.6.2. Statistical ineffective fault attacks	319
11.6.3. Lattice-based fault attacks	320
11.7. Countermeasures	321
11.7.1. Padding schemes	322
11.7.2. Verification, detection and infection	322
11.7.3. Attacks on countermeasures	323
11.8. Conclusion	324

11.9. Notes and further references	325
11.10. References	328
Chapter 12. Fault Countermeasures	333
Patrick SCHAUMONT and Richa SINGH	
12.1. Anatomy of a fault attack	333
12.2. Understanding the attacker	334
12.2.1. Fault attacker objectives	334
12.2.2. Fault attacker means	335
12.3. Taxonomy of fault countermeasures	336
12.4. Fault countermeasure principles	337
12.4.1. Redundancy	337
12.4.2. Randomness	338
12.4.3. Detectors	339
12.4.4. Safe-error defense	339
12.5. Fault countermeasure examples	340
12.5.1. Algorithm level countermeasures	340
12.6. ISA level countermeasures	342
12.7. RTL-level countermeasures	343
12.8. Circuit-level countermeasures	343
12.9. Design automation of fault countermeasures	344
12.10. Notes and further references	345
12.11. References	348
List of Authors	355
Index	357
Summary of Volume 2	363
Summary of Volume 3	371