

Contents

1	An Introduction to Timing Attacks	1
1.1	Side-Channel Attacks	3
1.1.1	Side-Channel Attack Requirements	4
1.1.2	The Attacker's Success	5
1.1.3	Side-Channel Attack Suppression	5
1.2	Timing Attacks	6
1.2.1	Kocher's Timing Attack	7
1.2.2	Taxonomy of Timing Attacks	9
1.3	Organization	10
	Reference	11
2	Modern Cryptography	13
2.1	Types of Encryption Algorithms	13
2.2	Block Ciphers: An Important Family of Symmetric-Key Ciphers	15
2.2.1	AES	16
2.2.2	CLEFIA	20
2.2.3	CAMELLIA	23
2.3	Classical Cryptanalysis	24
2.3.1	Classical Cryptanalysis of Block Ciphers	25
2.3.2	The Idea of Differential in Block Ciphers	25
2.4	Asymmetric-Key Ciphers	29
2.5	RSA: An Asymmetric-Key Algorithm	29
2.5.1	Square and Multiply Algorithm to Perform Exponentiation	30
2.6	Confinement Problem and Covert Channels	31
2.7	Formal Analysis of Side-Channel Attacks	32
2.8	Conclusion	33
	References	34
3	Superscalar Processors, Cache Memories, and Branch Predictors	37
3.1	Superscalar Processors	37
3.2	Memory Hierarchy and Cache Memory	39

3.2.1	Organization of Cache Memory	40
3.2.2	Improving Cache Performance for Superscalar Processors ..	43
3.3	Branch Prediction Unit	45
3.3.1	Static Branch Prediction	47
3.3.2	Dynamic Branch Prediction Schemes	47
3.3.3	Branch Target Buffers	50
3.4	Conclusion	50
	Reference	51
4	Time-Driven Cache Attacks	53
4.1	A Simple Illustration	53
4.1.1	Relation Between Size and Bits Revealed	55
4.1.2	Relation Between Alignment of Tables and Bits Revealed ...	56
4.1.3	Initial State of Cache Memory	56
4.2	Collisions from Execution Time	57
4.2.1	Clocks Using Hardware Time Stamp Counters	57
4.2.2	Clocks with Virtual Time-Stamp Counters	59
4.2.3	Distinguishing Cache Hit and Miss Events Using Time	60
4.3	Timing Attacks on Block Ciphers Based on Internal Collisions	63
4.3.1	Max, Min, or Max Deviation	65
4.4	Time-Driven Attack Based on Induced Cache Miss	66
4.5	Results	69
4.6	Conclusion	69
	Reference	69
5	Advanced Time-Driven Cache Attacks on Block Ciphers	71
5.1	Second Round Attack on AES	71
5.2	Differential Cache Attacks on Feistel Ciphers	72
5.3	Differential Cache Attack on CLEFIA	75
5.3.1	Differential Properties of CLEFIA's F Functions	75
5.3.2	Determining $RK0$ and $RK1$	76
5.3.3	Determining $WK0 \oplus RK2$ and $WK1 \oplus RK3$	77
5.3.4	Determining $RK4$ and $RK5$	78
5.3.5	Determining $RK2$ and $RK3$	79
5.4	Conclusion	79
	References	80
6	A Formal Analysis of Time-Driven Cache Attacks	81
6.1	Memory Access Model for a Block Cipher	81
6.2	Cache Misses in a Block Cipher	82
6.3	Average Execution Time of a Block Cipher	85
6.3.1	Estimating the Difference of Means	87
6.4	DOM as a Security Metric	88
6.5	Application of the Model	90

6.5.1	Comparing Cipher Implementations	91
6.5.2	Choosing the Right Implementation	92
6.6	Conclusion	94
7	Profiled Time-Driven Cache Attacks on Block Ciphers	95
7.1	Bernstein's Cache Timing Attack	95
7.1.1	Building a Timing Profile	95
7.1.2	Extracting Keys from Timing Profiles	97
7.2	Causes of Information Leakage	98
7.3	Quantifying Information Leakage in a Timing Profile	103
7.4	Information Leakage due to Hardware Prefetching	104
7.5	Conclusion	108
	References	108
8	Access-Driven Cache Attacks on Block Ciphers	109
8.1	Access-Driven Attacks on Block Ciphers	109
8.1.1	Second Round Access-Driven Attack on AES	112
8.1.2	A Last Round Access-Driven Attack on AES	112
8.2	Asynchronous Access-Driven Attacks	113
8.3	Secretly Monopolizing the CPU scheduler	114
8.3.1	Cheat Server	118
8.3.2	Binary Instrumentation	119
8.4	Fine Grained Access-Driven Attack on AES	119
8.5	Attack Procedure	120
8.5.1	Completely Fair Scheduler	120
8.5.2	Denial of Service Exploiting Completely Fair Scheduler	121
8.5.3	Using Timing as Side Channel for Cache Access Attack	122
8.5.4	Denoising by Neural Network	123
8.6	Conclusion	123
	References	124
9	Branch Prediction Attacks	125
9.1	Implementation of RSA	125
9.1.1	Square and Multiply Exponentiation Algorithm	125
9.1.2	Balanced Montgomery Powering Ladder Implementation	126
9.1.3	Montgomery Multiplication	126
9.2	Timing Branch Mispredictions	127
9.3	Attacking the Square and Multiply Exponentiation Algorithm	130
9.4	Asynchronous Attack on the Square and Multiply Algorithm	134
9.5	Synchronous Attack on the Square and Multiply Algorithm	136
9.6	Trace Driven Attack Targeting the BTB	136
9.7	Conclusion	137
	Reference	137

10 Countermeasures for Timing Attacks	139
10.1 Application Level Countermeasures	139
10.1.1 Countermeasures Involving Look-Up Tables	140
10.1.2 Data-Oblivious Memory Access Pattern	142
10.1.3 Constant and Random Time Implementations	142
10.2 Countermeasures Applied in the Hardware	143
10.2.1 Noncached Memory Accesses	143
10.2.2 Specialized Cache Designs	143
10.2.3 Specialized Instructions	144
10.2.4 Hardware Prefetching	145
10.2.5 Fuzzifying Clocks	145
10.3 Countermeasures in the Operating System	146
10.4 Conclusion	147
References	147
Appendix A: CPUs Used for Experiments	151

Timing Channels in Cryptography

A Micro-Architectural Perspective

Rebeiro, C.; Mukhopadhyay, D.; Bhattacharya, S.

2015, XVII, 152 p. 75 illus., 14 illus. in color., Hardcover

ISBN: 978-3-319-12369-1