

Contents

- Introduction.** 1
- Yong Guan, Sneha Kumar Kasera, Cliff Wang and Ryan M. Gerdes
- 1 Overview 1
- 2 Applications and Requirements of Fingerprints 2
- 3 Types of Fingerprints 2
- Types and Origins of Fingerprints.** 5
- Davide Zanetti, Srdjan Capkun and Boris Danev
- 1 Introduction 5
- 2 Physical-Layer Device Identification 6
 - 2.1 General View 6
 - 2.2 Device Under Identification 8
 - 2.3 Identification Signals 9
 - 2.4 Features 9
 - 2.5 Device Fingerprints 12
 - 2.6 Physical-Layer Identification System 13
 - 2.7 System Performance and Design Issues 14
 - 2.8 Improving Physical-Layer Identification Systems 15
- 3 State of the Art. 17
 - 3.1 Transient-Based Approaches 17
 - 3.2 Modulation-Based Approaches 21
 - 3.3 Other Approaches 22
 - 3.4 Attacking Physical-Layer Device Identification 23
 - 3.5 Summary and Conclusion 24
- 4 Future Research Directions. 25
- 5 Conclusion 26
- References 27

Device Measurement and Origin of Variation	31
Ryan M. Gerdes, Mani Mina and Thomas E. Daniels	
1 Introduction	31
1.1 ABCD Parameters	33
1.2 Proposed Model	33
2 Measuring Parameters	34
3 Determining Component Significance.	36
3.1 Constructing Model Input	36
3.2 Producing Model Output	36
3.3 Evaluating Model Output	37
4 Conclusion	38
References	38
Crypto-Based Methods and Fingerprints	39
Joe H. Novak, Sneha Kumar Kasera and Yong Guan	
1 Introduction	39
1.1 Authentication	39
1.2 Key Generation	40
2 Techniques	41
2.1 Physical Unclonable Functions	41
2.2 Controlled Physical Unclonable Functions	49
2.3 Clock Skew	52
2.4 Wireless Devices	58
2.5 Optical Media	61
2.6 Trojan Detection	63
2.7 Software Control	63
3 Tradeoffs	64
3.1 Benefits	64
3.2 Drawbacks	65
4 Summary	65
References	66
Fingerprinting by Design: Embedding and Authentication	69
Paul L. Yu, Brian M. Sadler, Gunjan Verma and John S. Baras	
1 Background	69
1.1 Intrinsic Fingerprints	69
1.2 Fingerprint Embedding	70
1.3 Fingerprinting and Communications	71
2 Introduction to Embedded Authentication.	72
3 Framework for Embedded Authentication	72
3.1 Authentication System—Transmitter	73
3.2 Authentication System—Receiver	74
3.3 Authentication Performance	77
4 Metrics for Embedded Fingerprint Authentication	77
4.1 Impact on Data BER	77
4.2 Authentication Performance	78

4.3	Security Analysis	79
4.4	Complexity	81
5	Experimental Results	82
5.1	Authentication Performance	82
5.2	Key Equivocation	82
5.3	Impact on Data BER	84
6	Conclusions	85
	Appendix: Precoding and Power-Allocation with CSI	85
	No CSI	85
	Perfect CSI	86
	Statistical CSI	86
	References	87
	Digital Fingerprint: A Practical Hardware Security Primitive	89
	Gang Qu, Carson Dunbar, Xi Chen and Aijiao Cui	
1	Introduction	89
2	Digital Fingerprinting for IP Protection	93
2.1	Background on Fingerprinting	93
2.2	The Need and Challenge of Digital Fingerprinting IPs	94
2.3	Requirements of Digital Fingerprinting	94
2.4	Iterative Fingerprinting Techniques	95
2.5	Fingerprinting with Constraint-Addition	98
3	Observability Don't Care Fingerprinting	100
3.1	Illustrative Example	100
3.2	Observability Don't Care Conditions	101
3.3	Finding Locations for Circuit Modification Based on ODCs	101
3.4	Determining Potential Fingerprinting Modifications	102
3.5	Maintaining Overhead Constraints	103
3.6	Security Analysis	103
4	Satisfiability Don't Care Fingerprinting	104
4.1	Satisfiability Don't Care and Illustrative Example	104
4.2	Assumptions for SDC Based Fingerprinting	105
4.3	SDC Based Fingerprinting Technique	106
4.4	Fingerprint Embedding Scheme	107
4.5	Security Analysis	108
5	Scan Chain Fingerprinting	109
5.1	Illustrative Example	109
5.2	Basics on Scan Chain Design	110
5.3	Scan Chain Fingerprinting	111
5.4	Security Analysis	111
6	Conclusion	113
	References	113

Operating System Fingerprinting	115
Jonathan Gurary, Ye Zhu, Riccardo Bettati and Yong Guan	
1 Overview of Operating System Fingerprinting	115
2 Major Operating System Fingerprinting Techniques	116
2.1 OS Fingerprinting	116
2.2 Reconnaissance Through Packet-Content Agnostic Traffic Analysis	122
2.3 Analysis of Smartphone Traffic	123
2.4 Analysis of Encrypted Traffic	124
3 Case Study: Smartphone OS Reconnaissance	124
3.1 System and Threat Model	127
3.2 Identifying Smartphone Operating Systems	128
3.3 Empirical Evaluation	132
4 Summary and Future Directions	135
Appendix A: Detailed Descriptions of Algorithms	136
References	137
 Secure and Trustworthy Provenance Collection for Digital Forensics	141
Adam Bates, Devin J. Pohly and Kevin R.B. Butler	
1 Introduction	141
2 Provenance-Aware Systems	142
2.1 Disclosed Provenance-Aware Systems	143
2.2 Automatic Provenance-Aware Systems	144
3 Ensuring the Trustworthiness of Provenance	147
3.1 Security Challenges to Provenance Collection	147
3.2 The Provenance Monitor Concept	149
4 High-Fidelity Whole Systems Provenance	150
4.1 Design of Hi-Fi	150
4.2 Handling of System-Level Objects	151
4.3 Hi-Fi Implementation	154
4.4 Limitations of Hi-Fi	158
5 Linux Provenance Modules	159
5.1 Augmenting Whole-System Provenance	159
5.2 Threat Model	160
5.3 Design of LPM	161
5.4 Deploying LPM	164
6 Analyzing the Security of Provenance Monitors	165
6.1 Completeness Analysis of Hi-Fi	165
6.2 Security Analysis of LPM	169
7 Current and Future Challenges to Provenance for Forensics	171
References	173

Conclusion 177

Yong Guan, Sneha Kumar Kasera, Cliff Wang and Ryan M. Gerdes

1 Overview 177

2 Measurements of Fingerprints 178

3 Fingerprints and Crypto-Based Methods. 179

4 Science of Fingerprints. 179

5 Security of Fingerprints 180

Index 183

Digital Fingerprinting

Wang, C.; Gerdes, R.M.; Guan, Y.; Kasera, S.K. (Eds.)

2016, IX, 189 p. 46 illus., Hardcover

ISBN: 978-1-4939-6599-1