

Contents

- 1 Introduction 1
- 2 What Do We Need to Know?
 - Techniques for Recording Platform State 3
 - 2.1 Recording Code Identity 3
 - 2.2 Recording Dynamic Properties 9
 - 2.3 Which Property is Necessary? 10
- 3 Can We Use Platform Information Locally? 13
 - 3.1 Secure Boot 13
 - 3.2 Storage Access Control Based on Code Identity 14
- 4 Can We Use Platform Information Remotely? 19
 - 4.1 Prerequisites 19
 - 4.2 Conveying Code Measurement Chains 19
 - 4.3 Privacy Concerns 22
- 5 How Do We Make Sense of Platform State? 25
 - 5.1 Coping With Information Overload 25
 - 5.2 Focusing on Security-Relevant Code 25
 - 5.3 Conveying Higher-Level Information 32
- 6 Roots of Trust 35
 - 6.1 General-Purpose Tamper-Resistant and Tamper-
Responding Devices 35
 - 6.2 General-Purpose Devices Without Dedicated
Physical Defenses 37
 - 6.3 Special-Purpose Minimal Devices 38
 - 6.4 Research Solutions Without Hardware Support 39
- 7 Challenges in Bootstrapping Trust in Secure Hardware 41
 - 7.1 Problem Definition 42
 - 7.2 Potential Solutions 45
 - 7.3 Preferred Solutions 50
- 8 Validating the Process 51
- 9 Applications 53
 - 9.1 Real World 53
 - 9.2 Research Proposals 55
- 10 Implementing Trust Bootstrapping: Open Source Tools 59
 - 10.1 Component Packages 59
 - 10.2 Complete Distributions or LiveCDs 60

11	Human Factors & Usability	61
11.1	Trustworthy Verifier Devices	61
11.2	Using Your Brain to Check a Computer	71
11.3	Pairing Two Trustworthy Devices	71
12	Limitations	73
12.1	Load-Time Versus Run-Time Guarantees	73
12.2	Hardware Attacks	73
13	Additional Reading	75
13.1	Books	75
13.2	Conference and Workshop Proceedings	76
14	Summary	77
	References	79
	Index	97