CONTENTS IN DETAIL

FOREWORD xvii

ACKNOWLEDGMENTS xix

INTRODUCTION xxi

The State of Embedded System Security xxii
Emerging Requirements, Laws, and Standards xxiii
Who Should Read This Book? xxiv
What Does This Book Cover? xxiv
A Note on the Case Studies in This Book xxv

PART I
FUNDAMENTALS

1
SECURE DEVELOPMENT PROCESS **3**

On the Variety of Guidelines 4
Responsibility for Product Security 5
Awareness and Training 6
Assets and Protection Goals 7
    Valuable Product Parts 7
    Relevant Protection Needs 8
Attackers, Threats, and Risks 11
    Potential Adversaries 11
    Potential Negative Impacts 13
    No Risks, No Priorities 14
Security Requirements and Security Architecture 16
    Risk Treatment 16
    Secure Development Principles 17
Secure Implementation and Security Testing 18
    Shift Left 18
    Continuous Testing and Analysis 19
    Attackers as a Service 21
Vulnerability Monitoring and Response 22
    Reporting Vulnerabilities 22
    Reviewing and Assessing Vulnerability Reports 23

Fixing or Addressing the Issue 23
Testing 23
Disclosing the Solution 23
Avoiding Future Issues 24
Establishing Trust 24
Summary 25

2
CRYPTOGRAPHY 27

Kerckhoffs's Principle 28
Levels of Security 28
Symmetric Ciphers 29
Data Encryption Standard 29
Advanced Encryption Standard 30
Modes of Operation 32
Electronic Codebook Mode 32
Cipher Block Chaining Mode 33
Counter Mode 34
Hash Functions 35
Message Authentication Codes 36
Authenticated Encryption 37
Strategies and Requirements 37
Galois Counter Mode 38
Asymmetric Cryptography 40
The RSA Cryptosystem 41
Basic RSA Math 41
Real-World RSA Usage 43
Diffie-Hellman Key Exchange 43
The Mathematical Beauty 44
Man-in-the-Middle Attacks 44
Elliptic-Curve Cryptography 45
The Math Behind the Curves 45
The Agony of Choice 47
Practical Applications of ECC 47
Summary 48

PART II
DEVICE SECURITY BUILDING BLOCKS

3
RANDOM NUMBER GENERATORS 51

The Need for Randomness 52
The Nature of Randomness 52

True Random Number Generators 53
Ring Oscillators 54
The Health Status of Entropy Sources 55
Pseudorandom Number Generators 56
Practical RNG Constructions and Usage 57
RNG Selection 57
Error Handling 57
Boot-Time Entropy 57
Case Study: Random Numbers from Hardware to Python 58
Hardware RNG and Entropy Source 58
Hardware RNG Integration in Linux 58
Linux RNG Architecture 59
Cryptographically Secure Random Numbers in Python 62
Case Study: Practical Tools for a Randomness Quick Check 63
Simple Tools for Distribution Analysis and Pattern Recognition 63
Problem 1: Output Space Restriction by Modulo 65
Problem 2: Custom PRNG Designs 66
Summary 67

4
CRYPTOGRAPHIC IMPLEMENTATIONS 69

Implementation Context and Requirements 70
Selecting Crypto Implementations 71
AES Implementation Options 73
Basic Architecture 73
Optimized Operations 73
Implementation Characteristics of RSA and ECDSA 74
RSA Optimizations 74
ECDSA Specifics 75
Case Study: Crypto Performance on an STM32MP157F Device 75
Parameter Choice for Symmetric Encryption 76
Software vs. Hardware Implementation for SHA-256 Hashing 78
Comparison of Software Performance of Asymmetric Crypto 81
Summary 83

5
CONFIDENTIAL DATA STORAGE AND SECURE MEMORY 85

Confidential Data 86
The Dilemma of Keeping Secrets on Embedded Systems 87
Secure Filesystem Approaches 87
Encrypted Stacked Filesystems 88
Native Filesystem Encryption 88
Encrypted Block Devices 88
Recommendations 89
The Passphrase 89

Secure Memory in Hardware . . . 89
External Secure Memory . . . 90
Internal Secure Memory . . . 91
Secrets in Application Code . . . 91
Secure Password Storage . . . 93
Case Study: Encrypted File Containers on Linux . . . 93
Crypto Benchmarking . . . 94
Container Creation . . . 95
Efficiency Analysis . . . 97
Read-Out Protection as a Low-Cost Solution . . . 98
Summary . . . 99

6
SECURE DEVICE IDENTITY 101

Every Device Is Unique . . . 102
Identification and Identifiers . . . 102
Unique Identifiers . . . 102
System Identities . . . 103
Authentication and Authenticators . . . 103
Authentication Protocols . . . 104
Dedicated Authentication Chips . . . 105
Multifactor Authentication . . . 105
Trusted Third Parties . . . 106
Certificates and Certificate Authorities . . . 107
Identity Life Cycle and Management . . . 107
Generation . . . 108
Provisioning . . . 109
Usage in the Field . . . 110
Exchange or Destruction . . . 110
Case Study: Identity Generation and Provisioning . . . 111
Identifiers and System Identity . . . 111
Certificate Signing Request . . . 113
Certificate Authority . . . 115
Case Study: RSA Key Generation in Production . . . 117
Summary . . . 118

7
SECURE COMMUNICATION 121

All the Protection Goals . . . 122
Transport Layer Security . . . 122
History . . . 123
TLS Basics . . . 124
TLS 1.3 . . . 124
TLS 1.2 . . . 126

Requirements for Devices and Infrastructure 127
Application Examples and Software Libraries 128
Case Study: Secure MQTT Communication 129
Mosquitto Installation and Configuration 129
The First Test Run 130
Communication Security Analysis with Wireshark and SSLyze 131
Secure Communication Without TLS 135
Redundancy in Secure Communication 136
Summary 137

PART III
ADVANCED DEVICE SECURITY CONCEPTS

8
SECURE BOOT AND SYSTEM INTEGRITY 141

System Boot Complexity 142
Boot Protection Concepts 143
Classic Secure Boot Chain 145
Considerations for Implementing Secure Boot 146
Hardware and Software Requirements 147
Development Process 147
Production and Lifetime 148
Open Source Licenses vs. Secure Boot 148
Case Study: Secure Boot Process on an STM32MP157F Device 149
The Boot Process 149
Secure Boot Starts in Hardware 150
Secure Boot Based on BL2 TF-A 151
U-Boot's Secure Boot Feature 152
Integrity Protection Beyond the Boot Process 154
Kernel Module Verification 154
Filesystem Integrity 155
Write Protection as a Low-Cost Solution 156
Summary 157

9
SECURE FIRMWARE UPDATE 159

The Inevitability of Updates 160
Security Requirements 161
Authenticity 161
Confidentiality 161
Secure Distribution Channel 161
Rollback Option 161
Version Distribution Monitoring 162

Distribution and Deployment of Updates 162
Local vs. Remote Updates 162
Pull vs. Push Strategy 163
Update Granularity and Format 163
Firmware Parts 164
Update Formats 165
Issues with Package Managers 166
Device Partitioning Strategies 166
Update/Recovery Partition 166
A/B System Approach 167
A Note on Updating Bootloaders 168
The Interplay Between Development, Backend, and Device 169
Case Study: Secure Firmware Updates with SWUpdate 170
SD Card Layout Customization 170
SWUpdate Installation and Configuration 171
Device-Specific Customization 174
Update Process Evaluation 177
Summary 179

10
ROBUST DEVICE ARCHITECTURE 181

Devices Under Network Stress 182
Malfunctioning Neighbor Devices 182
Protocol Fuzzing 182
Network and Vulnerability Scanning 182
Flooding Attacks 183
Robust Architectures 183
Essential Device Functions 183
Sensors 183
Actuators 184
Controllers 184
Real-Time Systems 185
Soft Real-Time Systems 185
Firm Real-Time Systems 185
Hard Real-Time Systems 185
Impact of DoS Attacks 186
Resource Exhaustion and Prevention Strategies 186
Hardware-Level Implementation Options 187
Dedicated Preprocessing Unit 187
Multicore Architectures 188
Operating System Capabilities 189
Operating System Options 189
Linux with a Real-Time Patch 190
Application and Protocol Considerations 190
Identify Logical Flaws 191
Implement Input and Sender Validation 191

Analyze Active Protection Measures 191
Introduce Chaos Engineering and Fuzzing 192
Case Study: Robustness Options on an STM32MP157F Device 192
Basic System Properties 192
Measurements on a Low-Latency Kernel 193
Measurements on a Real-Time Kernel 194
Real-Time Coprocessor 196
Summary 197

11
ACCESS CONTROL AND MANAGEMENT 199

Everyday Threats 200
Access Control and Damage Containment 201
Design and Development Phase 201
Production Considerations 202
Customer Activities and Decommissioning 203
Discretionary Access Control 203
Linux Filesystem Permissions 204
Linux User and Group Management 205
Linux Permission Management 206
Access-Control Lists 206
Case Study: Access Control for STM32MP157F-DK2 Firmware 207
User Creation and File Provisioning in Yocto 207
Exploration of System Files and Predefined Users 209
SSH Daemon Access-Control Configuration 210
Mandatory Access Control 211
Linux Security Modules 212
SELinux 212
AppArmor 213
Other LSMs and Non-LSM MACs 214
Case Study: Application Confinement with AppArmor 214
Installation 215
Application Profiling 218
Summary 221

12
SYSTEM MONITORING 223

Monitoring for the Right Reasons 224
Monitoring the Right Things 225
User Interactions and Access Control 225
Communication 226
Application Behavior 226
System Behavior 227
Risk-Based Monitoring 227

Designing a Monitoring Scheme 228
Challenges for Embedded Systems 228
Monitoring of the On-Device Logging Process 230
Central Log Analysis and Management 230
Case Study: Logging Events on an STM32MP157F Device 231
User-Session Monitoring with journald 231
Kernel Event Monitoring with auditd 232
Service and Application Event Logging 234
Logging to a Remote Server 236
Summary 237

AFTERWORD 239

INDEX 241