

Contents

Part I Embedded Devices

1	An Introduction to Smart Cards and RFIDs	3
	Keith Mayes and Konstantinos Markantonakis	
1.1	Introduction	3
1.2	Application Requirements	5
1.2.1	Mobile Communications	5
1.2.2	Banking Cards	7
1.2.3	Passports	8
1.2.4	Satellite Pay-TV	9
1.2.5	Transport Ticketing	10
1.2.6	Product Tagging	11
1.2.7	Comparing Requirements	12
1.3	Contact and Contactless Smart Cards/RFIDs	13
1.3.1	Cards with Contacts	13
1.3.2	Contactless Smart Cards/RFIDs	14
1.3.3	APDU Communication	15
1.4	The Range of Smart Card Devices	16
1.4.1	Simple ID Tag/Card	16
1.4.2	Memory Tag/Card	17
1.4.3	Secured Memory Tag/Card	17
1.4.4	Secured Microcontroller ID/Tag	18
1.5	The Importance of Providing Attack/Tamper-Resistance	19
1.6	Mobile and NFC	20
1.7	Conventional Smart Card Lifecycle Management Processes.	21
1.8	Conclusion.	23
	References	24
2	Embedded DSP Devices	27
	Serendra Reddy	
2.1	Overview	28
2.2	Digital Signal Processing	29

- 2.2.1 The DSP Processor 30
- 2.2.2 The Real-Time DSP System 32
- 2.2.3 The FPGA in DSP 34
- 2.2.4 The ASIP in DSP 35
- 2.3 Embedded DSP Systems 36
 - 2.3.1 The Embedded DSP Architecture 37
 - 2.3.2 The Embedded DSP Processor and RISC 40
 - 2.3.3 Embedded DSP and Security 42
 - 2.3.4 Embedded DSP and the Mobile Phone 44
- 2.4 Discussion 46
- References 46

- 3 Microprocessors and Microcontrollers Security 49**
 - Chris Shire
 - 3.1 Microcontrollers and Microprocessors Security Needs. 49
 - 3.2 Historical Development. 51
 - 3.3 The Microprocessor 52
 - 3.3.1 32 Bit Microprocessor Designs. 53
 - 3.3.2 64 Bit Microprocessor Designs. 54
 - 3.3.3 RISCs and ARM 54
 - 3.4 Security Design of Embedded CPU Architectures. 56
 - 3.4.1 Security of Embedded CPU Memory 61
 - 3.4.2 Security of Embedded CPU Interfaces 64
 - 3.5 Advanced Chip Design 65
 - 3.6 Conclusion. 67
 - References 68

- 4 An Introduction to the Trusted Platform Module and Mobile Trusted Module 71**
 - Raja Naeem Akram, Konstantinos Markantonakis and Keith Mayes
 - 4.1 Introduction 71
 - 4.2 The Trusted Platform Module 72
 - 4.2.1 Trusted Platform Framework 72
 - 4.2.2 Basic Architecture 73
 - 4.3 TPM Operations. 76
 - 4.3.1 TPM Endorsement Key. 76
 - 4.3.2 TPM Ownership. 77
 - 4.3.3 Attestation Identity Keys. 78
 - 4.3.4 Measurement and Reporting Operations 79
 - 4.3.5 Migration Model 83
 - 4.4 The Mobile Trusted Module 85
 - 4.4.1 Basic Architecture and Operations 85
 - 4.5 TPM/MTM Technology Contenders 88
 - 4.5.1 ARM TrustZone. 88

- 4.5.2 M-Shield 88
- 4.5.3 GlobalPlatform Device 88
- 4.5.4 Trusted Personal Devices. 89
- 4.5.5 Secure Element 89
- 4.5.6 Comparative Analysis of TPM/MTM Technology
Contenders. 89
- 4.5.7 What Lies Ahead? 91
- 4.6 Conclusion. 91
- References 92

- 5 Hardware and VLSI Designs 95**
- Mario Kirschbaum and Thomas Plos
- 5.1 Introduction and Motivation. 96
- 5.2 VLSI Design Cycle. 97
- 5.3 Design Space of Hardware Circuits 100
- 5.4 Secure Hardware Design 102
- 5.4.1 Power Consumption of CMOS Gates 103
- 5.4.2 Countermeasures Against Power-Analysis Attacks . . . 104
- 5.4.3 Verification of Countermeasures by Means
of Simulations 107
- 5.5 Instruction-Set Extensions 108
- 5.6 A 32-Bit Processor with ISEs and SCA Countermeasures . . . 110
- 5.7 Testability and Security. 112
- 5.8 Hardware Trojans 113
- 5.9 Conclusion and Summary 114
- References 115

Part II Generic Security and Processing Platforms

- 6 Information Security Best Practices 119**
- Keith Mayes and Konstantinos Markantonakis
- 6.1 Introduction 119
- 6.1.1 What is Information Security
and Who are the Adversaries? 120
- 6.2 Security Objectives. 121
- 6.2.1 Data Assets 122
- 6.2.2 Critical Functions 122
- 6.2.3 The Range of Security Protection. 122
- 6.3 Cryptographic Algorithms 123
- 6.3.1 Symmetric Algorithms 124
- 6.3.2 Asymmetric Algorithms 132
- 6.3.3 Other Algorithms/Modes 134

6.4	Key/Trust Management	135
6.4.1	Asymmetric Key Management	136
6.4.2	Trust and Management	137
6.5	Security Evaluation and Common Criteria	138
6.6	Handling Imperfection	139
6.7	Case Study the MIFARE Classic	140
6.7.1	Impact	141
6.8	Concluding Remarks	142
	References	143
7	Smart Card Security	145
	Michael Tunstall	
7.1	Introduction	145
7.2	Cryptographic Algorithms	147
7.2.1	Data Encryption Standard	147
7.2.2	RSA	149
7.3	Smart Card Security Features	152
7.3.1	Communication	153
7.3.2	Cryptographic Coprocessors	154
7.3.3	Random Number Generators	154
7.3.4	Anomaly Sensors	155
7.3.5	Chip Features	155
7.4	Side Channel Analysis	157
7.4.1	Timing Analysis	157
7.4.2	Power Analysis	158
7.4.3	Electromagnetic Analysis	163
7.4.4	Countermeasures	164
7.5	Fault Analysis	166
7.5.1	Fault Injection Mechanisms	166
7.5.2	Modelling the Effect of a Fault	167
7.5.3	Faults in Cryptographic Algorithms	168
7.5.4	Countermeasures	171
7.6	Embedded Software Design	172
7.6.1	PIN Verification	172
7.6.2	File Access	174
7.7	In Conclusion	175
	References	175
8	Graphics Processing Units	179
	Peter Schwabe	
8.1	An Introduction to Modern GPUs	180
8.1.1	NVIDIA GPUs	180
8.1.2	AMD GPUs	183
8.1.3	Programming GPUs in High-Level Languages	183

- 8.1.4 Programming GPUs in Assembly 185
- 8.1.5 GPU Performance Bottlenecks 185
- 8.2 GPUs as Cryptographic Coprocessors 187
 - 8.2.1 AES on GPUs 188
 - 8.2.2 Asymmetric Cryptography on GPUs 190
- 8.3 GPUs in Cryptanalysis 192
- 8.4 Malware Detection on GPUs 194
- 8.5 Malware Targeting GPUs 195
- 8.6 Accessing GPUs from Web Applications 196
- References 197

9 A Survey of Recent Results in FPGA Security and Intellectual Property Protection 201

François Durvaux, Stéphanie Kerckhof, Francesco Regazzoni and François-Xavier Standaert

- 9.1 FPGAs: An Overview 202
 - 9.1.1 Structure 202
 - 9.1.2 Design Flow 204
 - 9.1.3 Technologies 205
- 9.2 Security IPs 205
 - 9.2.1 The AES Case 206
 - 9.2.2 Performance Evaluation 209
 - 9.2.3 Side-Channel Attacks and Countermeasures 210
 - 9.2.4 Fault Attacks and Countermeasures 212
- 9.3 IP Security 213
 - 9.3.1 Bitstream Security 213
 - 9.3.2 Design Security 214
- 9.4 Conclusions 219
- References 220

Part III Applications and Platform Embedded Security Requirements

10 Mobile Communication Security Controllers 227

Keith Mayes and Konstantinos Markantonakis

- 10.1 Introduction 227
- 10.2 An Overview of the SIM 229
 - 10.2.1 The SIM in Operation 230
- 10.3 Security Analysis 232
 - 10.3.1 Categories of Cellular Usage 232
 - 10.3.2 The Roles in Communication Solutions 233
- 10.4 Security Fundamentals 236
 - 10.4.1 Trust Operations 237

- 10.4.2 Initialisation, Personalisation and Key Management 238
- 10.4.3 Authentication/Encryption 238
- 10.4.4 Management of SIM Data and Application 239
- 10.4.5 Migration 239
- 10.4.6 Extended Operations/Value-Added Service Management 240
- 10.4.7 NFC Management 240
- 10.5 Generic Attacks on Smart Cards. 241
 - 10.5.1 Logical Attacks 241
 - 10.5.2 Physical Attacks 242
 - 10.5.3 Side Channel Attacks 244
 - 10.5.4 Fault Attacks 246
 - 10.5.5 Summary and Main Points. 246
- 10.6 SIM Implementation Options 247
 - 10.6.1 Pure Software SIM 247
 - 10.6.2 Hardware Shared Security Software SIM Solution (HS-SSIM) 249
 - 10.6.3 Standalone HW Security SIM Solution 251
- 10.7 Trusted Platform. 254
 - 10.7.1 Roots of Trust 255
 - 10.7.2 Authenticated Boot and Secure Storage. 256
 - 10.7.3 Ownership 256
 - 10.7.4 Mobile Trusted Platform (MTP). 257
- 10.8 Summary. 260
 - 10.8.1 Value Added Service Management. 263
 - 10.8.2 Concluding Remarks. 264
- References 265
- 11 Security of Embedded Location Systems 267**
 - G. P. Hancke
 - 11.1 Introduction 267
 - 11.2 Embedded Location Systems 268
 - 11.3 Security and Resilience of Location Information 270
 - 11.3.1 Security and Resilience of Position Estimation Methods 273
 - 11.4 Securing Position Estimation Methods 277
 - 11.5 Global Navigation Satellite Systems 280
 - 11.5.1 GPS Security 280
 - 11.5.2 Future Efforts on Securing GNSS. 283
 - 11.6 Conclusion. 284
 - References 284

12 Automotive Embedded Systems Applications and Platform

Embedded Security Requirements. 287
 Jan Pelzl, Marko Wolf and Thomas Wollinger

12.1 Introduction: Smart Embedded Platform Automotive 287

 12.1.1 Smart Communication Platform 289

 12.1.2 Smart After-Market Platform 290

 12.1.3 Smart Future Platform. 290

12.2 Security Aspects of Smart Embedded Automotive
 Platforms. 291

 12.2.1 Automotive Attackers 292

 12.2.2 Automotive Attack Paths. 292

 12.2.3 Automotive Security Threats and Risks. 296

 12.2.4 Security of Automotive Safety Mechanisms. 296

 12.2.5 Security of Automotive Legal Applications 298

 12.2.6 Security of Automotive Business Models 298

 12.2.7 Automotive Privacy Aspects 299

 12.2.8 Real-World Automotive Security Incidents 299

 12.2.9 Examples of Automotive Security Mechanisms 300

12.3 Smart and Secure Open Automotive Platforms Platform 302

 12.3.1 OVERSEE Virtualisation. 302

 12.3.2 OVERSEE Security Services Architecture. 304

 12.3.3 OVERSEE Security Implementation. 306

12.4 Conclusions 308

References 308

13 Analysis of Potential Vulnerabilities in Payment Terminals 311
 Konstantinos Rantos and Konstantinos Markantonakis

13.1 Introduction 311

 13.1.1 EMV Standard 314

13.2 Current Terminal Status 316

 13.2.1 Types of Terminals. 316

 13.2.2 Where does Security Apply? 317

13.3 Types of Attacks 320

 13.3.1 Attacking the Supply Chain. 320

 13.3.2 Exploiting Inadequate Security Measures 322

 13.3.3 Skimming 324

 13.3.4 Covert Channels to PINs. 325

 13.3.5 PIN/PIN Block Interception and Cracking. 326

 13.3.6 Manipulating the Terminal-Card Interface 327

 13.3.7 Relay Attacks. 330

13.4 Conclusions and Future Considerations 331

References 332

- 14 Wireless Sensor Nodes 335**
 Serge Chaumette and Damien Sauveron
 - 14.1 Introduction 335
 - 14.2 Applications. 336
 - 14.3 Constraints. 337
 - 14.3.1 Costs: Production Versus Performance 337
 - 14.3.2 Energy 338
 - 14.3.3 Management: Self and Decentralized 339
 - 14.4 Architecture and Operating System. 339
 - 14.4.1 Sensing Unit 340
 - 14.4.2 Processing Unit 341
 - 14.4.3 Communication Unit. 342
 - 14.4.4 Major Features of Operating Systems 342
 - 14.5 Security Concerns. 343
 - 14.5.1 Security of Wireless Sensor Nodes 343
 - 14.5.2 Security in Networks of Wireless Sensor Nodes. 345
 - References 347

- 15 Near Field Communication 351**
 Gerald Madlmayr, Christian Kantner and Thomas Grechenig
 - 15.1 Introduction 351
 - 15.2 NFC Technology 352
 - 15.2.1 Physical Layer 352
 - 15.2.2 Use Cases and Applications. 354
 - 15.3 Hardware Integration 355
 - 15.3.1 NFC Chip 355
 - 15.3.2 Secure Element 356
 - 15.3.3 Host Controller 357
 - 15.4 NFC and Linux 359
 - 15.5 NFC Integration in Android. 359
 - 15.5.1 NFC Chip 360
 - 15.5.2 API for the NFC Chip. 361
 - 15.5.3 API for the Secure Element Access 362
 - 15.5.4 Security. 362
 - 15.6 NFC Tags 364
 - 15.6.1 Tag-Types 364
 - 15.6.2 NFC Data Exchange Format (NDEF) 364
 - 15.7 Conclusion. 366
 - References 366

- 16 The BIOS and Rootkits 369**
 Graham Hili, Keith Mayes and Konstantinos Markantonakis
 - 16.1 The BIOS 369
 - 16.1.1 The BIOS Subsystem Functionality 370

- 16.2 Attacks on the BIOS Subsystem. 371
 - 16.2.1 Countermeasures to BIOS Attacks 373
- 16.3 Rootkits. 373
 - 16.3.1 Introduction to Rootkits. 373
- 16.4 Rootkit Infections. 374
 - 16.4.1 Detection of Rootkits 376
 - 16.4.2 Removal of Rootkits. 378
- 16.5 Conclusion. 379
- References 379

- 17 Hardware Security Modules 383**
 - Sathis Mavrovouniotis and Mick Ganley
 - 17.1 Introduction 383
 - 17.2 HSM Usage 384
 - 17.3 HSM Physical Security 388
 - 17.4 HSM Security Evaluation and Approvals. 389
 - 17.5 HSM Management 393
 - 17.6 Key Management 395
 - 17.7 Command Manipulation Attacks. 399
 - 17.8 Conclusions 403
 - References 404

- 18 Security Evaluation and Common Criteria 407**
 - Tony Boswell
 - 18.1 Introduction 407
 - 18.2 Security Evaluation Issues 408
 - 18.2.1 The Security Evaluation Model 412
 - 18.2.2 Structure and Use of the Common Criteria 413
 - 18.2.3 Structure of Common Criteria 415
 - 18.2.4 Assurance Requirements and Assurance Levels 416
 - 18.2.5 CC Interpretation and Supporting Documents 416
 - 18.2.6 Attack Potential Calculations 417
 - 18.3 Evolution of Common Criteria 418
 - 18.3.1 CC Technical Communities 419
 - 18.3.2 New Generation Protection Profiles 420
 - 18.4 Other Security Evaluation Schemes 420
 - 18.4.1 FIPS 140. 421
 - 18.4.2 PCI PIN Transaction Security Requirements 422
 - 18.5 Example Protection Profiles. 423
 - 18.5.1 Security IC PP. 423
 - 18.5.2 Payment Terminal (Point of Interaction) PP set 424
 - 18.5.3 Trusted Platform Module PP 425
 - References 426

19 Physical Security Primitives 429
 Ahmad-Reza Sadeghi, Steffen Schulz and Christian Wachsmann

19.1 Introduction 429

19.2 Physically Unclonable Functions 431

 19.2.1 PUF Concept and Properties 431

 19.2.2 PUF Types 432

 19.2.3 Noise Compensation and Privacy Amplification. 435

 19.2.4 Characterizing the Unpredictability of PUFs 436

19.3 Attacks Against PUFs and PUF-Based Systems 437

 19.3.1 Emulation Attacks 437

 19.3.2 Side-Channel Attacks 437

 19.3.3 Fault Injection Attacks 438

19.4 Advanced PUF Concepts 438

 19.4.1 Controlled PUFs. 439

 19.4.2 Emulatable PUFs 439

19.5 Common Applications of PUFs 440

 19.5.1 Device Identification and Authentication. 440

 19.5.2 Secure Key Storage and Key Generation. 441

19.6 Future Directions 441

 19.6.1 Logically Reconfigurable PUFs 441

 19.6.2 PUF-Based Remote Attestation 442

19.7 Open Questions and Challenges 443

19.8 Conclusion. 444

References 445

20 SCADA System Cyber Security. 451
 Igor Nai Fovino

20.1 Introduction 451

20.2 SCADA Architecture Overview 452

 20.2.1 SCADA Protocols Overview 453

20.3 SCADA Vulnerabilities and Attacks 455

 20.3.1 Architectural Vulnerabilities 456

 20.3.2 Security Policy Vulnerabilities 457

 20.3.3 Software Vulnerabilities 459

 20.3.4 Communication Protocol Vulnerabilities 459

20.4 SCADA Security Countermeasures 460

 20.4.1 Communication Protocol Countermeasures 461

 20.4.2 Filtering Coutermeasures 462

 20.4.3 Monitoring Coutermeasures 464

 20.4.4 General Architectural Best Practices 465

20.5 Conclusion. 469

References 469

Part IV Practical Examples and Tools

21 An Overview of PIC Microcontrollers and Their Suitability for Cryptographic Algorithms. 475
 Mehari G. Msgna and Colin D. Walter

21.1 Introduction 475

21.2 Microcontroller Structure. 476

21.3 Peripheral Interface Controllers 477

 21.3.1 PIC Architecture. 477

 21.3.2 Memory 478

 21.3.3 Other Components 479

 21.3.4 Development Tools. 479

 21.3.5 Summary. 480

21.4 AES on a PIC 480

 21.4.1 Implementation of AES. 481

21.5 Attack Example 482

 21.5.1 Differential Power Analysis. 483

 21.5.2 Practical Implementation of DPA. 485

21.6 Conclusion. 493

References 493

22 An Introduction to Java Card Programming. 497
 Raja Naeem Akram, Konstantinos Markantonakis
 and Keith Mayes

22.1 Introduction 497

22.2 Smart Card Programming 498

 22.2.1 Smart Card Architecture 498

 22.2.2 Smart Card Hardware 499

 22.2.3 Communication Architecture 500

 22.2.4 Application Development Lifecycle 502

22.3 Java Card 503

 22.3.1 Java Card Classic 503

 22.3.2 Java Card Connected 504

22.4 Java Card Programming 506

 22.4.1 Java Card Applet Architecture 506

22.5 My First Applet 507

 22.5.1 Application Design 507

 22.5.2 Coding 509

 22.5.3 Simulating and Testing 511

22.6 Conclusion. 512

References 512

23 A Practical Example of Mobile Phone Application

Using SATSA (JSR 177) API 515

Lishoy Francis

23.1 Introduction 515

 23.1.1 A Brief Overview of SATSA Framework 517

 23.1.2 A Brief Overview of Java Card Framework. 518

23.2 Practical Example. 518

 23.2.1 Developing a MIDP Application (MIDlet)

 Implementing SATSA APDU Communication API . . 518

 23.2.2 Developing a Java Card Applet 525

 23.2.3 Results: Testing MIDlet and Java Card Applet. 531

23.3 Conclusion. 532

 23.3.1 Source Code of MIDP Application (MIDlet) 533

 23.3.2 Source Code of Java Card Applet. 535

 23.3.3 Java Card Applet Download-Script. 537

References 539

24 Wireless Sensors (Languages/Programming/Developments Tools/Examples) 541

J r mie Albert, Lionel Barr re, Serge Chaumette and Damien Sauveron

24.1 Introduction 541

24.2 Sun SPOTs (Sun Small Programmable Object Technology). . . 542

 24.2.1 Introduction 542

 24.2.2 History 543

 24.2.3 Hardware Overview 543

 24.2.4 Software Overview 544

 24.2.5 How to Start with a Sun SPOT 544

 24.2.6 Hello World (“Shake and Blink”) 546

 24.2.7 Networked Sun SPOTs Applications. 548

24.3 Arduino. 550

 24.3.1 Introduction and History 550

 24.3.2 Hardware Overview 550

 24.3.3 Software Overview 551

 24.3.4 How to Start with a Arduino 552

 24.3.5 Hello World (“Blinking SOS”) 553

 24.3.6 Networked Arduino Application. 555

24.4 TinyOS 556

 24.4.1 Introduction 556

 24.4.2 Hardware Overview 557

 24.4.3 How to Start with TinyOS. 558

 24.4.4 Hello World (“Sense and Blink”). 559

 24.4.5 Networking with TinyOS. 560

24.5 Sensor Network Deployment: An Example 561

- 24.5.1 Introduction 561
- 24.5.2 Hardware Architecture 561
- 24.5.3 The Time Synchronization Issue. 562
- 24.5.4 Data Collection, Location and Network Load Issues. 563
- 24.5.5 The Problem of Missing Information 563
- 24.5.6 Conclusion. 564
- References 564

- Errata to: Secure Smart Embedded Devices,
Platforms and Applications E1**

- Index 565**



<http://www.springer.com/978-1-4614-7914-7>

Secure Smart Embedded Devices, Platforms and Applications

Markantonakis, K.; Mayes, D.K. (Eds.)

2014, XLI, 568 p. 135 illus., Hardcover

ISBN: 978-1-4614-7914-7