

Security In Embedded Devices

[DOWNLOAD HERE](#)

1;Security in EmbeddedDevices;1 1.1;Preface;4 1.2;1 Where Security Began;10 1.2.1;1.1 A Brief History of Cryptography;14 1.2.2;1.2 Brief History of the Side Channel;18 1.2.3;1.3 Summary;20 1.2.4;References;20 1.3;2 Introduction to Secure Embedded Systems;22 1.3.1;2.1 Contact Chip Card or Smart Card;26 1.3.2;2.2 Contactless SmartCards and RFID Tags;27 1.3.3;2.3 Cell Phones and PDAs;29 1.3.4;2.4 Automobiles;30 1.3.5;2.5 Game Stations;32 1.3.6;2.6 Satellites;33 1.3.7;2.7 FPGA, Networks on a Chip;33 1.3.8;2.8 Summary;34 1.3.9;References;35 1.4;3 The Key;37 1.4.1;3.1 Key Randomness;38 1.4.2;3.2 Physically Unclonable Functions;40 1.4.3;3.3 Key Lifetime, Freshness, Updating;43 1.4.4;3.4 Key Length;44 1.4.5;3.5 Key Storage and Authentication Issues;47 1.4.6;3.6 Key Types;48 1.4.7;3.7 Trusted Platform Module (TPM);49 1.4.8;3.8 Network on Chip Security;51 1.4.9;3.9 Summary;55 1.4.10;References;56 1.5;4 Using Keys;57 1.5.1;4.1 No Shared Keys;59 1.5.2;4.2 Using a Preexisting Shared Key;61 1.5.3;4.3 Using Keys in Conventional Crypto;62 1.5.3.1;4.3.1 Needham--Schroeder;64 1.5.3.2;4.3.2 Kerberos;65 1.5.4;4.4 Public Key Approaches;66 1.5.4.1;4.4.1 Protocols;67 1.5.4.1.1;4.4.1.1 Basic Encrypt;67 1.5.4.1.2;4.4.1.2 Digital Signature;68 1.5.4.1.3;4.4.1.3 Key Establishment, Certificates, and Protocols;70 1.5.4.2;4.4.2 Mathematics Behind PKC;72 1.5.4.2.1;4.4.2.1 Crypto Based on the Integer Factorization Problem;72 1.5.4.2.2;4.4.2.2 Crypto Based on Discrete Logarithm;76 1.5.5;References;81 1.6;5 Elliptic Curve Protocols;82 1.6.1;5.1 High-Level Elliptic Curve Computations;86 1.6.1.1;5.1.1 Performance Improvements;89 1.6.2;5.2 The Mathematics Behind Elliptic Curves;91 1.6.2.1;5.2.1 The Curve Over a Field;91 1.6.2.1.1;5.2.1.1 Prime Fields;92 1.6.2.1.2;5.2.1.2 Binary Fields;93 1.6.2.2;5.2.2 Point Computations;96 1.6.2.2.1;5.2.2.1 Point Computations Over Prime Field;97 1.6.2.2.2;5.2.2.2 Point Computations Over Binary Field;97 1.6.2.3;5.2.3 Improving Performance;100 1.6.2.3.1;5.2.3.1 Coordinate Representation;102 1.6.2.3.2;5.2.3.2 Field Computations;105 1.6.3;5.3 EC Protocols;107 1.6.4;5.4 Embedded Implications;112 1.6.5;References;114 1.7;6 Symmetric Key Protocols Including Ciphers;117 1.7.1;6.1 The Theory of a Cipher;117 1.7.2;6.2 Block Ciphers;121 1.7.2.1;6.2.1 Rijndael: The Advanced Encryption Standard;122 1.7.2.1.1;6.2.1.1 Sub Bytes Function;123 1.7.2.1.2;6.2.1.2 Shift Row Function;124 1.7.2.1.3;6.2.1.3 Mix Column Function;125 1.7.2.1.4;6.2.1.4 High-Speed AES Software

Implementation;127 1.7.2.2;6.2.2 CAST;128 1.7.2.3;6.2.3 TEA;130 1.7.2.4;6.2.4 HIGHT;131 1.7.2.5;6.2.5 PRESENT Cipher;133 1.7.3;6.3 Stream Ciphers;134 1.7.3.1;6.3.1 Stream Cipher Principles;135 1.7.3.2;6.3.2 RC4;137 1.7.3.3;6.3.3 Grain;138 1.7.4;6.4 Cipher Modes of Operation;139 1.7.5;6.5 Authenticated Modes for Encryption;142 1.7.6;6.6 Embedded Systems Implications;144 1.7.7;References;147 1.8;7 Data Integrity and Message Authentication;149 1.8.1;7.1 Properties of Hash and MAC;151 1.8.2;7.2 The Structure of Integrity and Authentication Functions;154 1.8.2.1;7.2.1 The SHA-2 Function;158 1.8.3;7.3 Integrity Trees;160 1.8.4;7.4 Embedded Implications;163 1.8.5;References;166 1.9;8 Side Channel Attacks on the Embedded System;168 1.9.1;8.1 The Side Channel;168 1.9.1.1;8.1.1 Theory of the Side Channel;169 1.9.1.2;8.1.2 The Side Channel Attack in Practice;171 1.9.1.2.1;8.1.2.1 EM Probe;173 1.9.1.2.2;8.1.2.2 The Oscilloscope;176 1.9.1.2.3;8.1.2.3 Device and Trigger;178 1.9.1.3;8.1.3 Setting up a SCA;179 1.9.2;8.2 What is Simple Analysis;181 1.9.3;8.3 Differential Analysis;184 1.9.4;8.4 Correlation Analysis;194 1.9.5;8.5 Differential Frequency Analysis;195 1.9.6;8.6 Experiments on PDAs;196 1.9.6.1;8.6.1 EM Results;200 1.9.6.1.1;8.6.1.1 SEMA of AES on the PDA;202 1.9.6.1.2;8.6.1.2 Truncated code Analysis of the PDA;208 1.9.6.1.3;8.6.1.3 Attack of the Device Using Full AES;214 1.9.7;8.7 Experiment EAN/ISBN : 9781441915306 Publisher(s): Springer, Berlin, Springer US Format: ePub/PDF Author(s): Gebotys, Catherine H.

[DOWNLOAD HERE](#)

Similar manuals:

[Security In Embedded Devices](#)