Table of Contents

Foreword v

Preface vii

Table of Contents xi

List of Figures xv

List of Tables xvii

List of Abbreviations xix

I The Preliminaries 1

1 Introduction 3

1.1 Hope for the Best, Prepare for the Worst 3

1.2 Outline 7

1.3 Summary of Research Contributions 9

2 Related Work 11

3 Brief Background in Security and Cryptography 13

3.1 Enforcing the Secrecy of Secrets 13

3.2 Symmetric-Key Cryptography 14

3.2.1 Data Encryption Standard 15

3.2.2 Advanced Encryption Standard 17

3.3 Asymmetric-Key Cryptography 19

3.3.1 Rivest Shamir Adleman 22

3.3.2 Elliptic Curve Cryptography 23

3.4 Recommended Key Lengths 26

3.5 Hash Functions 27

3.6 Message Authentication Codes 29
3.6.1 Block Cipher Based Message Authentication Codes 30
3.6.2 Hash Function Based Message Authentication Codes . . . 30
3.7 Cryptographic Implementations 31
3.7.1 Software Implementations 31
3.7.2 Hardware Implementations 32
3.8 Trusted Computing Technology 35
3.8.1 Trusted Computing Components 35
3.8.2 Trusted Computing Basic Functionalities 37
3.9 Security Schemes in the Automotive Domain 40
3.9.1 Digital Signatures 40
3.9.2 Key Exchange and Hybrid Encryption 41
3.9.3 Public-Key Infrastructure 43
3.9.4 Challenge-Response Protocol 44
3.10 Cryptanalysis 45

II The Threats 47

4 Security-Critical Vehicular Applications 49
4.1 Introduction 49
4.2 Theft Protection 49
4.2.1 Electronic Immobilizer 50
4.2.2 Remote Door Lock 51
4.3 Counterfeit and Intellectual Property Protection 53
4.3.1 Counterfeit Protection 53
4.3.2 Intellectual Property Protection 53
4.4 Software Updates 54
4.5 After-Sale Applications 56
4.5.1 Feature Activation 56
4.5.2 Infotainment 57
4.6 Legal Applications 58
4.6.1 Milage Counter 58
4.6.2 Electronic License Plate 59
4.6.3 Digital Tachograph 60
4.6.4 Event Data Recorder 61
4.6.5 Electronic Log Book 62
4.6.6 Road Pricing 62

4.7 Vehicular Communication 63
4.7.1 In-Vehicle Communication 63
4.7.2 Vehicle-to-Device Communication 64
4.7.3 Vehicle-to-Infrastructure Communication 66
4.7.4 Vehicle-to-Vehicle Communication 68
4.8 Protection of Safety-Critical Applications 71
4.9 Privacy Protection 73

5 Attackers and Attacks in the Automotive Domain 77
5.1 Attackers in the Automotive Domain 77
5.2 Attacks in the Automotive Domain 80
5.2.1 Logical Attacks 82
5.2.2 Physical Attacks 86
5.2.3 Further Attacks 88

6 Security Analysis and Characteristical Constraints in the Automotive Domain 91
6.1 Security Objectives Analysis 91
6.2 Security Requirements Engineering 94
6.3 Characteristical Advantages 97
6.4 Characteristical Constraints 98
6.4.1 Technical Constraints 99
6.4.2 Non-Technical Constraints 100

III The Protection 105

7 Vehicular Security Technologies 107
7.1 Physical Security 107
7.1.1 Tamper-Evidence 108
7.1.2 Tamper-Resistance 109
7.1.3 Tamper-Detection 110
7.1.4 Tamper-Response 110
7.2 Security Modules 110
7.2.1 Software Module 112
7.2.2 Security Controller 113
7.2.3 Trusted Platform Module 113
7.2.4 Security Box 115

7.3 Vehicular Security Architectures 115
7.3.1 Central Security Architecture 116
7.3.2 Distributed Security Architecture 117
7.3.3 Semi-Central Security Architecture 119

8 Vehicular Security Mechanisms **121**
8.1 Why Proper Security Application is Hard 121
8.2 Secure Component Identification 122
8.2.1 Cryptographic Component Identification 123
8.2.2 Physically Unclonable Functions 125
8.3 Secure User Authentication 125
8.4 Software Protection 128