

Kerstin Lemke · Christof Paar · Marko Wolf (Eds.)

# Embedded Security in Cars

Securing Current and  
Future Automotive IT Applications

With 53 Figures and 25 Tables

---

# Contents

---

## Part I Introduction

---

<b>Embedded IT Security in Automotive Application – An Emerging Area</b>	
<i>Christof Paar</i> .....	3

---

## Part II Security in the Automotive Domain

---

<b>Aspects of Secure Vehicle Software Flashing</b>	
<i>Winfried Stephan, Solveig Richter, Markus Müller</i> .....	17
<b>Secure Software Delivery and Installation in Embedded Systems</b>	
<i>André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi</i> .....	27
<b>Anti-theft Protection: Electronic Immobilizers</b>	
<i>Kerstin Lemke, Ahmad-Reza Sadeghi, Christian Stübke</i> .....	51
<b>A Review of the Digital Tachograph System</b>	
<i>Igor Furgel, Kerstin Lemke</i> .....	69
<b>Secure In-Vehicle Communication</b>	
<i>Marko Wolf, André Weimerskirch, Christof Paar</i> .....	95
<b>A Survey of Research in Inter-Vehicle Communications</b>	
<i>Jun Luo, Jean-Pierre Hubaux</i> .....	111

---

## Part III Embedded Security Technologies

---

<b>Fundamentals of Symmetric Cryptography</b>	
<i>Sandeep Kumar, Thomas Wollinger</i> .....	125

**Fundamentals of Asymmetric Cryptography**

*Thomas Wollinger, Sandeep Kumar* ..... 145

**Security Aspects of Mobile Communication Systems**

*Jan Pelzl, Thomas Wollinger* ..... 167

**Embedded Cryptography: Side Channel Attacks**

*Kai Schramm, Kerstin Lemke, Christof Paar* ..... 187

**Embedded Security: Physical Protection against Tampering Attacks**

*Kerstin Lemke* ..... 207

---

**Part IV Business Aspects of IT Systems in Cars**

---

**Automotive Digital Rights Management Systems**

*Marko Wolf, André Weimerskirch, Christof Paar* ..... 221

**Security Risks and Business Opportunities in In-Car Entertainment**

*Marcus Heitmann* ..... 233

**In-Vehicle M-Commerce: Business Models for Navigation Systems and Location-based Services**

*Klaus Rüdiger, Martin Gersch* ..... 247