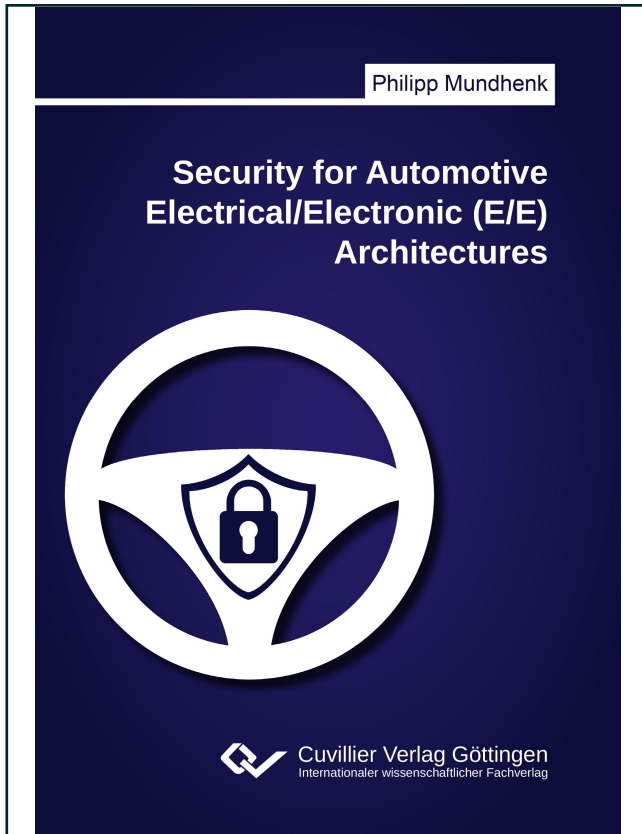




Philipp Mundhenk (Autor)
**Security for Automotive Electrical/Electronic (E/E)
Architectures**



<https://cuvillier.de/de/shop/publications/7598>

Copyright:

Cuvillier Verlag, Inhaberin Annette Jentsch-Cuvillier, Nonnenstieg 8, 37075 Göttingen, Germany
Telefon: +49 (0)551 54724-0, E-Mail: info@cuvillier.de, Website: <https://cuvillier.de>



Contents

Acknowledgements	i
Abstract	iii
Zusammenfassung (German Abstract)	v
1 Introduction	1
1.1 Automotive Electrical/Electronic (E/E) Architectures	2
1.1.1 Requirements	2
1.1.2 Computation	4
1.1.3 Current and Upcoming Networks	6
1.2 Security	9
1.2.1 Principles	10
1.2.2 Processes	11
1.2.3 Types of Cryptography	12
1.2.4 Algorithms	12
1.2.5 Evaluating Security	14
1.3 Automotive Security	16
1.3.1 External Security	16
1.3.2 Internal Security	17
1.3.3 Device Security	18
1.3.4 Standardization	18
1.3.5 Legal Situation	19
1.3.6 Attack Examples	20
1.3.7 Summary	22
1.4 Challenges	23
1.4.1 Design Time	23
1.4.2 Runtime	24
1.5 Contributions	25
1.6 Related Work	28
1.6.1 Automotive Threats	28



1.6.2	Intrusion Detection, Network Analysis & Verification	29
1.6.3	Encryption and Hardware Support	30
1.6.4	Security Integration	30
1.6.5	Other domains	31
1.6.6	Summary	31
1.7	Organization and Bibliographic Notes	32
2	Design Experience - EVA	35
2.1	Introduction and Summary	35
2.1.1	Summary	37
2.2	Architecture	37
2.3	Implementation	39
2.3.1	Central Server	39
2.3.2	Central Information Screen (CIS)	41
2.3.3	Instrument Cluster (IC)	42
2.3.4	Smartphones	43
2.4	Evaluation	43
2.4.1	Performance	44
2.4.2	Security	45
2.5	Concluding Remarks	47
3	Probabilistic Security Analysis for Automotive Architectures	49
3.1	Problem Description and Summary	49
3.2	Related Work	50
3.3	Framework	51
3.3.1	Problem Description	52
3.3.2	Analysis Flow	52
3.4	Methodology	54
3.4.1	Model Transformation	55
3.4.2	Component Assessment	57
3.4.3	Property Definition	58
3.5	Model Synthesis	60
3.6	Property Specification	65
3.7	Model Checking	66
3.8	Experimental Results	68
3.8.1	Architecture Evaluation	69
3.8.2	Parameter Exploration	71
3.8.3	Scalability	72
3.9	Concluding Remarks and Future Work	73



4	Lightweight Authentication Framework	75
4.1	Problem Description and Summary	75
4.1.1	Challenges and Opportunities	77
4.1.2	Contributions	78
4.2	Related Work	78
4.3	Authentication & Authorization	81
4.3.1	Terminology	81
4.3.2	ECU Authentication	81
4.3.3	Stream Authorization	83
4.4	Integration	85
4.4.1	Certificate Validation	85
4.4.2	System Life-Cycle Scenarios	86
4.4.3	System Setup	86
4.4.4	Vehicle Service	88
4.4.5	Firmware updates	89
4.5	Verification	89
4.6	Simulation	92
4.6.1	Model	92
4.6.2	Implementation	98
4.7	Evaluation	99
4.7.1	Simulator	99
4.7.2	LASAN	102
4.7.3	Security Comparison	104
4.7.4	Latency Comparison	106
4.8	Concluding Remarks and Future Work	110
5	Flexible and Reliable Message Scheduling in FlexRay	113
5.1	Problem Description and Summary	113
5.2	Related Work	116
5.3	Architecture	119
5.3.1	Runtime Scheduling Algorithm	119
5.3.2	Multi-Mode Applications	120
5.3.3	Wrapper PDUs	120
5.4	Design-Time Scheduling	121
5.4.1	Heuristic	124
5.4.2	Integer Linear Program (ILP)	126
5.5	Experimental Results	128
5.5.1	Size Variations	129
5.5.2	Latency	131
5.5.3	Period Variations	133



5.5.4	Computational Performance	135
5.6	Concluding Remarks and Future Work	136
6	Concluding Remarks	137
6.1	Future Work	139
	Bibliography	143
	List of Tables	159
	List of Figures	161
	Glossary	163