
Contents

1	Introduction	1
1.1	Motivation	2
1.2	Objective	3
1.2.1	What can be Evaluated Automatically During a Design Phase regarding the Exploitability Risk of Automotive On-Board Networks?	4
1.2.2	How to Efficiently Generate Attack Graphs?	5
1.2.3	What Other Attack Paths Exist, and What is the Total Risk for an Asset?	5
1.3	Thesis Outline	6
1.4	Resulting Contributions	6
1.4.1	Survey	7
1.4.2	System Model, Attacker Profile, and Exploit Model	8
1.4.3	Attack Surface Exploitability Quantification	9
1.4.4	Implementation and Evaluation of the Models and the Attack Surface Exploitability Quantification	9
1.4.5	Design of the Single-Path Attack Graph Algorithm	10
1.4.6	Implementation and Evaluation of the Single-Path Attack Graph Algorithm	11
1.4.7	Probabilistic Model for Overall Risk Computation	12
1.4.8	Design of the Multi-Paths Attack Graph Algorithm (P3Salfer)	12
1.4.9	Bayes Network Unsuitability Finding	13

1.4.10	Design and Implementation of an Alternative Algorithm with Bayesian Networks (P3Bayes)	13
1.4.11	Implementation and Evaluation of the Multi-Path Attack Graph Algorithm (P3Salfer)	13
2	Basics and Related Work	15
2.1	Typical Attacks against Automotive On-Board Networks	16
2.1.1	Typical Attack Surface	17
2.1.2	Typically Attacked Assets	17
2.1.3	Typical Techniques	18
2.1.4	Typical Attacker	21
2.1.5	Overall Situation	22
2.2	Automotive On-Board Networks	25
2.2.1	Connectivity Standards	26
2.2.2	Electronic Control Units / Cyber-Physical Systems	29
2.2.3	Development Requirements and Regulations	32
2.3	Exploitability Risk	39
2.3.1	Risk Assessment	39
2.3.2	Known Vulnerabilities	41
2.3.3	Attack Surface / Unknown Vulnerabilities	42
2.4	Stochastics	48
2.4.1	Bernoulli Trials and Processes	48
2.4.2	Gaussian Distribution	48
2.4.3	Bayes Theorem	51
2.4.4	Monte Carlo Methods	52
2.4.5	Error Quantification	52
2.5	Attack Graphs	53
2.5.1	Application	54
2.5.2	Origins and Trends of Attack Graphs	55
2.5.3	Attack Graph Types	58
2.5.4	Visualization	65
2.5.5	Graph Search Algorithms	67
2.5.6	Graph Construction and Generation	71
2.6	Model-Driven Security	81
2.6.1	Attacker Profiles	81
2.6.2	System Model	85
2.7	Summary	86

3	System Model, Attacker Profile, Exploit Model, Attack Graphs and Exploitability Quantification	87
3.1	Scope and Main Requirements	88
3.1.1	Applicability During the Design Phase and Beyond	89
3.1.2	Remote Code Execution Focus	89
3.1.3	Involvement of all ECUs	89
3.1.4	Real-World Usage	89
3.2	Notation	90
3.3	System Model	90
3.3.1	ECU	91
3.3.2	Software	92
3.3.3	Communication Medium	92
3.3.4	Asset	93
3.4	Attacker Profile	93
3.4.1	Motivation	95
3.4.2	Budget and Gaussian Random Variables	95
3.4.3	Skills	96
3.4.4	Access	97
3.4.5	Known Exploits	97
3.5	Exploit Model	97
3.6	Attack Surface Exploitability Quantification	99
3.6.1	Attack Surface Collection	99
3.6.2	Vulnerability Existence Probability	102
3.6.3	Vulnerability Finding Effort	104
3.6.4	Vulnerability Exploitation Effort	109
3.6.5	Exploitability Quantification Summary	112
3.7	Attack Graph Model	113
3.8	Implementation of the Proof of Concept	114
3.8.1	Requirements	114
3.8.2	Architecture and Technology Decisions	116
3.9	Evaluation and Discussion	119
3.9.1	Meeting the Requirements	120
3.9.2	Implementation Programming Language	121
3.9.3	Validity and Real-World Usage	122
3.10	Summary	129

4	Single-Path Attack Graph Algorithm	131
4.1	Scope and Main Requirements	132
4.1.1	Overall Network Exploitation Evaluation	132
4.1.2	Known Network Layout	133
4.1.3	Realistic Likelihood by Considering the Attack Economy	134
4.1.4	Automatic and Comprehensive Generation	134
4.2	Design of the Single-Path Attack Graph Algorithm	134
4.2.1	Phase I: Heuristics Preparation	135
4.2.2	Phase II: Single-Path Attack Graph Construction	135
4.2.3	Asymptotic Complexity	139
4.3	Implementation of the Single-Path Attack Graph Algorithm	140
4.4	Evaluation of the Proof of Concept	146
4.4.1	Meeting the Requirements	146
4.4.2	Runtime Optimization with Object Orientation	148
4.4.3	Performance Benchmark Method	148
4.4.4	Performance Benchmark Results	152
4.5	Summary	154
5	Multi-Path Attack Graph Algorithm	157
5.1	Scope and Main Requirement	159
5.2	Design of the Multi-Path Attack Graph Algorithm	159
5.2.1	Model Extension for Multi-Path Attack Graphs	160
5.2.2	Algorithm Steps	165
5.2.3	Termination Guarantee	168
5.2.4	Performance Considerations	168
5.2.5	Alternative Algorithm with Bayesian Networks (P3Bayes)	170
5.2.6	Avoiding Cycles	175
5.3	Implementation of the Multi-Path Attack Graph Algorithm	177
5.3.1	P3Salfer Implementation	177
5.3.2	P3Bayes Implementation	180
5.3.3	Automated Graph Visualization	189
5.3.4	Optimization	192
5.4	Evaluation of the Proof of Concept	194
5.4.1	Benchmarking Method	194
5.4.2	Results and Discussion	199
5.5	Summary	206

Contents	xv
6 Conclusion	209
List of Publications	213
Declaration on Competing Interests	217
References	219