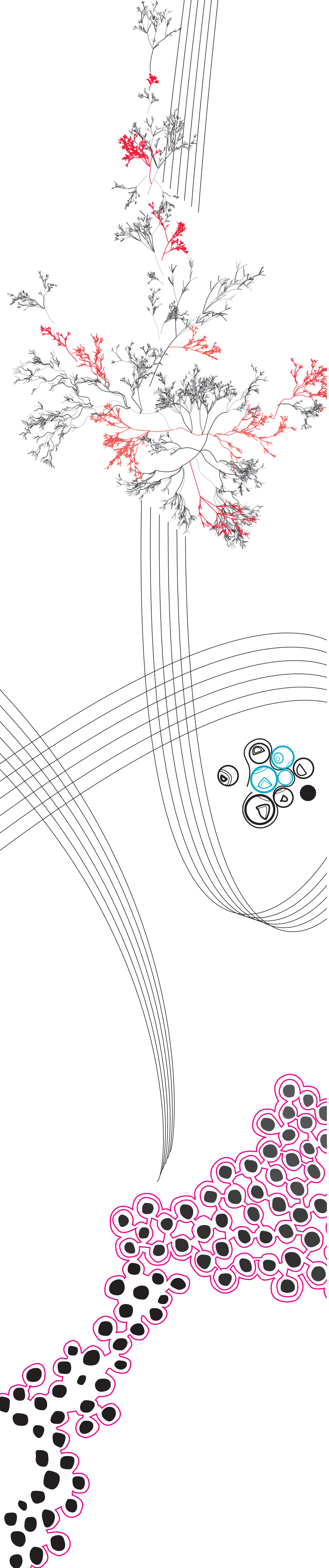

MASTER THESIS

PRACTICAL CYBER-ATTACKS ON AUTONOMOUS VEHICLES

Bas G.B. Stottelaar

Faculty of Electrical Engineering, Mathematics and Computer Science
Services, Cybersecurity and Security Research Group

Committee:
Prof. Dr. Frank Kargl
Prof. Dr. Ir. Raymond Veldhuis
Dr. Jonathan Petit
Dipl.-Inf. Michael Feiri

May 4, 2015
Version: 2123ddc

UNIVERSITY OF TWENTE.

ABSTRACT

This thesis explores the field of Autonomous Vehicle (AV) sensor technologies and potential cyber-attacks on sensors. The research on AVs is increasing tremendously, as the first vehicles are due to hit the road by 2020. Unfortunately, the literature on cyber-attacks on AVs is limited and theoretical. The first part of this work addresses the available sensor technologies, including limitations, attacks and countermeasures. Examples of sensor technologies include Laser Image Detection and Ranging (Lidar), Tire-pressure Monitoring System (TPMS) and Global Navigation Satellite System (GNSS). In the second part of this thesis, practical attacks on the hardware layer of Lidar and camera sensors will be demonstrated on actual hardware (MobilEye C2-270 Advanced Driver Assistance System (ADAS) and ibeo LUX 3 Lidar system). Camera-related attacks include blinding and auto controls confusion attacks. The Lidar attacks include jamming, relaying and spoofing attacks. The attacks are evaluated according to an external attacker model with limited money and knowledge. The experiments are proof-of-concept, and are conducted in a lab environment. It was found that the MobilEye C2-270 is sensitive to low-cost near-infrared light sources, but these light sources cannot blind it. However, a low-budget low-power visible lasers can. The Lidar was susceptible to jamming, relay and spoofing attacks using low-cost hardware. Counterfeit signals can also influence the tracking software. Three examples of the impact of the attacks on the application level have also been shown, including an attack on sensor fusion. The last section of this work discusses several countermeasures that can mitigate or limit the demonstrated attacks.

ACKNOWLEDGEMENTS

Without the enthusiasm of my supervisors I would never haven chosen this topic. Their way of thinking helped me a lot, and got me through the easy and hard times. When I first contacted Jonathan and Michael to talk about this thesis topic, I was told that it would be hard and that the outcome would be unknown. Nevertheless, it would be a very practical topic and the result would be eye-opening. Thanks to you guys, I got the possibility to challenge myself and show what I could do. I hope that I have properly wrote down all the practical things I did.

Furthermore, many thanks to my girlfriend Mirjam, family and friends for supporting and providing feedback. Even though my due date changed many, many, many times, you still kept believing in what I did, even in hard times. This will mark the end of my study career at the University of Twente. Special thanks to Dirk, Kevin, Lambert, Marijn and Ties for helping me to improve the text. I have concluded that I am better at writing program code than text.

Also, many thanks to Geert Jan Laanstra. He provided me a place to work for more than one year, and his knowledge was valuable while reverse engineering the Lidar, doing the measurements and debating camera countermeasures. It is also thanks to him that I can still use my eyes. Playing with lasers can be very dangerous!

Finally, I would like to thank V-Tron B.V. in Deventer and Ibeo Automotive Systems GmbH in Hamburg for providing the MobilEye C2-270 and ibeo LUX 3 to experiment with. Without their generosity, this work would not have been possible. I had fun playing with the devices and find attack possibilities while simultaneously reverse engineering the hardware in terms of operation.

CONTENTS

1 INTRODUCTION 1
1.1 Problem statement 1
1.2 Research questions 2
1.3 Contributions 3
1.4 Organization 3

2 DEFINITIONS AND ATTACKER MODEL 5
2.1 Degrees of Automation 5
2.2 Cyber-attacks 6
2.2.1 Definition 6
2.2.2 Types of attack 7
2.3 Attacker model 8
2.4 Attack scenarios 11

3 AUTONOMOUS VEHICLE SENSORS 13
3.1 Sensor Technologies 13
3.1.1 Lidar 14
3.1.2 GNSS 17
3.1.3 Camera 27
3.1.4 TPMS 33
3.2 Sensor Fusion 36
3.2.1 Kalman Filter 36
3.2.2 Particle Filter 39
3.2.3 Attacks 45
3.2.4 Countermeasures 46

4 ATTACKING AUTONOMOUS VEHICLE SENSORS 47
4.1 Camera 48
4.1.1 Calibrating the hardware 49
4.1.2 Testing sensitivity 50
4.1.3 Blinding the camera 57
4.1.4 Confusing the auto controls 62
4.2 Lidar 67
4.2.1 Interfacing the hardware 67
4.2.2 Understanding the Lidar 69
4.2.3 Jamming the signal 74
4.2.4 Relaying the signal 79
4.2.5 Spoofing the signal 80
4.3 Conclusions 85

5 DISCUSSION 87
5.1 Impact on application level 87
5.1.1 Camera 87
5.1.2 Lidar 88
5.1.3 Sensor fusion 89
5.2 Countermeasures 92
5.2.1 Camera 92
5.2.2 Lidar 95
5.3 Limitations 97

6 CONCLUSIONS AND FUTURE WORK 101
6.1 Summary 101
6.2 Research questions 102
6.3 Future work 104
6.3.1 Camera 105
6.3.2 Lidar 105
6.3.3 Application level 106
6.3.4 Countermeasures 106

A SENSOR FUSION: A CASE STUDY 107
A.1 Kalman Filter 107
A.2 Particle Filter 109

B SPECTROMETRY 113

C RESULTS OF CAMERA EXPERIMENTS 117
C.1 Testing sensitivity 117
C.2 Blinding the camera 121
C.3 Confusing the auto controls 132

D OVERVIEW OF HARDWARE 141
D.1 MobilEye C2-270 141
D.2 ibeo LUX 3 142
D.3 Light sources 143
D.3.1 Infrared 143
D.3.2 Spots 144
D.3.3 Lasers 145
D.4 Cameras 146
D.5 Measurement tools 147
D.6 Other 148

ACRONYMS 151

BIBLIOGRAPHY 153

LIST OF FIGURES

Figure 1 Problem statement on external sensing 2
Figure 2 Example of an attack tree 9
Figure 3 Lidar perception of the world 15
Figure 4 Three-dimensional view of a Lidar 16
Figure 5 Dilution of precision in GNSS 20
Figure 6 x-y plot of GPS points 20
Figure 7 Sensor fusion with Emap 22
Figure 8 Visual overlay of Emap algorithm 23
Figure 9 CWI inference from a car GPS jammer 24
Figure 10 Adaptive Notch filtering applied to CWI 26
Figure 11 Example of rolling shutter effect 28
Figure 12 Multiband image capturing example 29
Figure 13 Result of thresholding an image 30
Figure 14 Common Haar-like features 31
Figure 15 Simplified setup of stereoscopic vision 31
Figure 16 Example of a Dazzler weapon and beam 32
Figure 17 Laser damaged CMOS sensor 33
Figure 18 Front and back of a TPMS sensor 34
Figure 19 Mean, K-window and Kalman filtering compared 37
Figure 20 Flowchart of a KF 38
Figure 21 Flowchart of a PF 40
Figure 22 Posterior, prior and likelihood relation 41
Figure 23 PF applied to robot localization problem 44
Figure 24 Ambiguity in a PF with two and three beacons 45
Figure 25 MobilEye C2-270 installed in a car 48
Figure 26 MobilEye C2-270 SeeQ Camera Calibration Tester 50
Figure 27 Sensitivity of an eye compare to image sensors 51
Figure 28 Inverse-square law of light sources 53
Figure 29 Setup of light sensitivity test 54
Figure 30 650 nm laser @ 50 cm 55
Figure 31 850 nm LED @ 50 cm 55
Figure 32 860 nm LED @ 50 cm 56
Figure 33 Effects of auto controls 57
Figure 34 Setup of blinding experiment 58
Figure 35 White Spot in light @ 50 cm 58
Figure 36 850 nm Spot in light @ 50 cm 59
Figure 37 940 nm 5x5 LED Matrix in dark @ 200 cm 59
Figure 38 365 nm spot in light @ 100 cm 63
Figure 39 White spot in light @ 50 cm 64
Figure 40 940 nm 5x5 LED matrix in dark @ 100 cm 64
Figure 41 Typical test setup of the ibeo LUX 3 68
Figure 42 Screenshot of Ibeo Laser View Premium 68
Figure 43 Lidar pattern visualized 70
Figure 44 Angular resolution of Lidar 70
Figure 45 Measuring angular resolution 71
Figure 46 Setup of Lidar mirror experiment 72
Figure 47 Result of Lidar mirror experiment 72
Figure 48 Result of Lidar mirror experiment 73

Figure 49 Setup of Lidar glass experiment 73
Figure 50 Result of the Lidar glass experiment 74
Figure 51 Setup of Lidar patterns visualization 75
Figure 52 Visualization of three Lidar pulses 76
Figure 53 Visualization of one Lidar pulse 77
Figure 54 Setup of a Lidar jamming attack 77
Figure 55 Lidar jamming signal visualized 78
Figure 56 Lidar jamming parameters 78
Figure 57 Lidar jamming attack 79
Figure 58 Setup of a Lidar relay attack 80
Figure 59 Lidar relay attack 80
Figure 60 Setup of a Lidar injection attack 81
Figure 61 Result of the Lidar injection attack 82
Figure 62 Lidar spoofing parameters 82
Figure 63 Result of the Lidar spoofing attack 83
Figure 64 Result of the Lidar spoofing attack 83
Figure 65 Tracking identification number over time 84
Figure 66 Lidar attack window 84
Figure 67 MobilEye live blinding experiment 88
Figure 68 Second MobilEye live blinding experiment 88
Figure 69 ibeo LUX 3 live experiment 89
Figure 70 Spoofing the PF with alternating beacons 90
Figure 71 Spoofing the PF with moving beacons 91
Figure 72 Spoofing the PF with random beacons 92
Figure 73 Combined setup of spectrometer and camera. 94
Figure 74 Illustration of image channel separation 95