Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR

Jonathan Petit[†*]
jpetit@securityinnovation.com

Bas Stottelaar[†], Michael Feiri[†]
basstottelaar@gmail.com
m.feiri@utwente.nl

Frank Kargl[†‡]
frank.kargl@uni-ulm.de

[*]Security Innovation
Wilmington, MA
United States

[†]Services, Cybersecurity and Safety
University of Twente
The Netherlands

[‡]Institute of Distributed Systems
University of Ulm
Germany

ABSTRACT

Autonomous automated vehicles are the next evolution in transportation and will improve safety, traffic efficiency and driving experience. Automated vehicles are equipped with multiple sensors (LiDAR, radar, camera, etc.) enabling local awareness of their surroundings. A fully automated vehicle will unconditionally rely on its sensors readings to make short-term (i.e. safety-related) and long-term (i.e. planning) driving decisions. In this context, sensors have to be robust against intentional or unintentional attacks that aim at lowering sensor data quality to disrupt the automation system. This paper presents remote attacks on camera-based system and LiDAR using commodity hardware. Results from laboratory experiments show effective blinding, jamming, replay, relay, and spoofing attacks. We propose software and hardware countermeasures that improve sensors resilience against these attacks.

Keywords

Security, automated vehicle, remote attack, LiDAR, camera

1. INTRODUCTION

Autonomous automated vehicles (for the sake of clarity shortened to Automated Vehicle (AV) in this paper) are getting close to market. The SAE J3016 [32] defined different levels of automation (from zero to five), in which Level 5 means that all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver are performed by the automation system, and this, potentially without driver present in the vehicle. However, automated vehicles can only work properly with accurate, reliable and trustworthy sensors. Therefore, AVs are equipped with a multitude of sensors, using different physical properties (light, ultrasound, radio frequency, etc.), Global Navigation Satellite System and accurate road maps. Successful examples of AVs are the Stanford Shelley [19], AnnieWAY [34] or the Google Driverless Car [9]. All of them use Light Imaging Detection and Ranging (LiDAR) to detect objects and camera for traffic sign recognition and delineation, influencing the overall mission planning. Indeed, when the LiDAR detects an obstacle on the road, the mission is re-planned to avoid that object. LiDAR and camera are the only sensors based on light, capable of 3D representation and "reading", which make LiDAR and camera essential for proper functioning of AVs.

In that context, resilience of AV sensors against attacks is a key challenge. Indeed, any attack that degrades sensor data can cause false driving reaction (or at Level 1-2 automation, fake warning that would distract the driver), leading potentially to accidents and fatalities [29]. For example, if camera is attacked and fooled, it can misread a speed limit sign, leading to unsafe driving conditions for the vehicle's passengers. If a LiDAR detects a fake obstacle because of an attack and triggers an emergency brake, it will seriously alter traffic efficiency if done at a large scale.

Contributions: In this paper, we present attacks on camera and LiDAR systems. As we think the most realistic type of attacker will be outside of the target vehicle, we only consider remote attacks. To assess the feasibility and sophistication of the attacks, we only use commodity hardware (below 60 US$) and perform black-box attacks. Results show successful blinding, jamming, replay and spoofing attacks in different laboratory conditions.

Organization: Section 2 presents the related work in the domain of automotive security. Section 3 details the system attacked. Section 4 describes the attacker model considered. Section 5 and 6 present attacks on the camera MobilEye C2-270 and LiDAR ibeo LUX 3, with their respective countermeasures. Section 7 highlights the limitations of our experiments, while Section 8 concludes the paper and presents future work.

2. RELATED WORK

Security analysis of modern automotive systems, especially in-vehicle networks, is a well-researched topic [16, 22]. Wolf et al. [36] investigated attacks of automotive bus systems (LIN, CAN, MOST, FlexRay, Bluetooth) assuming that an attacker has physical or logical access to the corresponding vehicle network. Hoppe et al. [12] demonstrated practical

CAN bus attacks where an attacker can manipulate electric window lifts, warning lights and the airbag control system. Koscher et al. [18] demonstrated that an attacker who is able to infiltrate virtually any Electronic Control Unit (ECU) can leverage this ability to completely circumvent a broad array of safety-critical systems. They demonstrated the ability to impose hostile control over a wide range of automotive functions and completely ignore driver input – including disabling the brakes, selectively braking individual wheels on demand, and stopping the engine.

Checkoway et al. [6] analyzed the external attack surface of a modern automobile. They discovered that remote exploitation is feasible via a broad range of attack surfaces (including mechanics tools, CD players, Bluetooth and cellular radio), and further, that wireless communications channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft.

Petit and Shladover [29] listed attack surfaces on automated and connected vehicles with their respective potential cyber-attacks. LiDAR and Camera are listed as attack surfaces but no detail on how to perform attacks were given.

We differentiate from the aforementioned work by performing real experiments on automated vehicle sensors to check feasibility and sophistication of remote attacks.

3. SYSTEM MODEL

The automation system of automated vehicles follows three phases depicted in Figure 1 (i.e. 'Sense', 'Understand', 'Act'). First, the AV senses its surroundings using a set of sensors. Then, from these raw sensors data, it constructs a representation of its environment by fusing them. Finally, the 'action engine' decides the appropriate actions to take (e.g. warn driver, manipulate vehicle controls). In this paper, we focus on the 'Sense' phase because sensor fusion algorithms cannot fully work properly with poor (or accurate but fake) raw sensor data [27].

As highlighted in Section 1, camera and LiDAR sensors are essential for proper functioning of AVs, and were selected for four reasons. First, existing automated vehicles make extensive use of LiDAR and camera as a source of information for perception. Secondly, in The Netherlands, the use of sensors such as RADAR, tire pressure sensors and GNSS use licensed radio frequency and would require a license to perform our attacks. Thirdly, camera and LiDAR can be used in laboratory environment for controlled experiments, without being integrated in an actual vehicle. Fourthly, attacks on TPMS [31] and GNSS [4] have already been demonstrated in real experiments.

3.1 Camera: MobilEye C2-270

A camera is an optical device that can perceive the world as a digital video signal. It is used in automated vehicles for lane detection [3], horizon/vanishing point detection [17], object detection and tracking (vehicles, pedestrians) [7, 15], traffic sign recognition [24], headlight detection [37], terrain classification [35]. Most applications share a common task: extract interesting regions from an image (segmentation), extract features from these regions and classify them with common classifiers such as AdaBoost classifiers or Support Vector Machines.

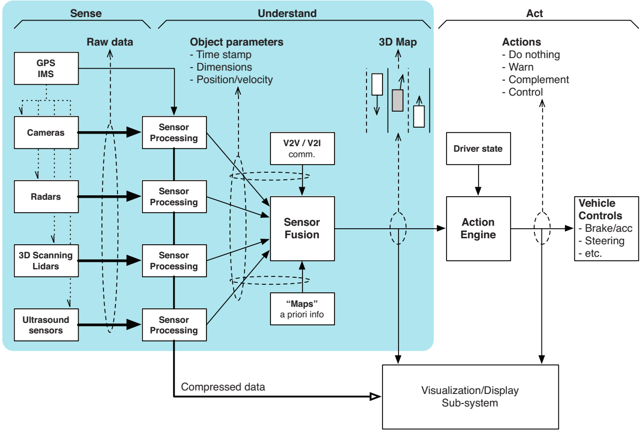


Figure 1: A functional view of the data flow in an autonomous car's sensing and control system [25].

Image quality is the most important parameter of camera-based systems and the context of moving automated vehicles brings its set of challenges. Indeed, the image quality is affected by lenses, windshield, vibration, and environmental conditions (e.g. light, rain, snow), potentially causing objects to get unnoticed, or increasing processing time for image correction [20]. Hence, one option is to rely on multiple cameras. For example, the VisLab's BRAiVE automated vehicle has ten cameras installed [5], including ones in the side mirrors, which are regularly calibrated to minimize the distortion between cameras. Another option is to use better optical systems to provide sharper pictures, enhance performance in low light conditions and reduce glare. For instance, in [14], multi-band images were used to improve images quality by capturing far-infrared images (700 nm - 1200 nm) together with normal images (400 nm - 700 nm), allowing better distinction of scene objects when light is limited, such as during the night. However, one should note that these options require additional space, demand additional processing capacities, and increase cost, which is problematic in the highly cost-driven automotive context.

The camera system used in this paper is the MobilEye C2-270 [23]. It is an Advanced Driver Assistance System (ADAS) that assists the driver in four tasks: headway monitoring and warnings, pedestrian collision warning, lane departure warning, intelligent headlight control (i.e. automatically dim the headlights in the dark when incoming traffic is detected). This system is based on one camera, which is installed on the windshield, under the rear view mirror (see Figure 2). It is noteworthy that this system is not sold specifically for full vehicle automation (SAE Level 5), but for function-specific vehicle automation (SAE Level 1-2-3).

3.2 LiDAR: ibeo LUX 3

For vehicle guidance and road safety, the acquisition of the geometry of all objects on and around the road is required [30]. Image-based acquisition typically requires good lighting conditions (e.g. day time and weather). It cannot robustly provide precise object geometry information under poor condi-

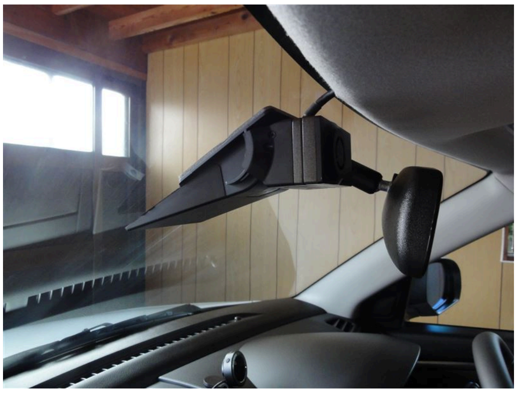


Figure 2: MobilEye C2-270 installed (on the windshield) with the display at the bottom.

tions. Advances in laser scanning technology led to LiDAR that has proven to be very efficient in acquiring very dense point clouds (over 800 points per square meter) along road corridors. The data acquired by laser scanners can be used to robustly capture the geometry of the road environment and be the basis for the recognition of a wide range of objects. A detailed classification of objects, in particular traffic signs and road lanes will, however, remain largely based on camera.

LiDAR is a type of range-finding sensor that emits light pulses and measures the time it takes to reflect off a distant surface, called a *ping*. These laser pulses are commonly bounced off of a spinning mirror thousands of times per second, creating a scan of laser pulses. When the original pulse is received more than once, these additional pulses received are called *echoes*. Echoes are useful to detect objects under almost any weather condition.

LiDAR is commonly used for Adaptive Cruise Control (ACC), Collision Avoidance System (CAS) [10] and object recognition. When a LiDAR sensor is mounted on a rotatable mirror, it can be used to provide vision in two or three dimensional view. LiDAR provides a spatial resolution of 10 cm, which enables accurate scanning that can classify pedestrians and cars [21]. One way to classify objects, is by using a depth map. For instance, a pedestrian will appear as a small object on the depth map, while a car will appear as a much bigger object. Combined with speed information and tracking algorithms, objects can be classified and tracked.

The LiDAR tested in this paper is the ibeo LUX 3 [13]. It is a four-layer laser-based ranging system, mounted on a rotating head to provide view up to 110°. The four layers refer to the number of scanning rays. Each layer is slightly tilted with respect to the road, so the LiDAR can operate on uneven roads (e.g. bumpy roads, hills, etc.). Even though it is a multi-layer LiDAR, it cannot provide a three-dimensional view, but only four layers of two-dimensional planes. The maximal range is up to 200 meters, depending on the weather conditions and it can detect up to three echoes. The minimal constant angular resolution between pulse is 0.25° at 12.5Hz or 25Hz, and 0.5° at 50Hz. For instance, at 20 m and 50Hz, the gap between each pulse would be 0.29 m wide.

The ibeo LUX 3 contains an embedded object tracking system that uses a Kalman Filter to track the following objects: car, truck, bike, pedestrian, unknown small, unknown big, non classified. The maximum number of objects that can be tracked is 65. Each object, when detected, is augmented with an object identification number for tracking purposes.

4. ATTACKER MODEL

Following the attacker model described in [28], we consider an external attacker that targets sensor data acquisition. Indeed, as seen in Section 3, AVs strongly rely on accurate sensor data. Thus, in this paper, we focus on attacks that aim at degrading sensors data quality. The attacker considered has limited resources (time to perform the attack—attack should be brief—and money) with the intention of *actively* (i.e. will send signal) disrupting components *undetectably* (i.e. no damage to device, leave no trace, not detectable by law enforcement) and *externally* (i.e. remotely). The type of attack should require low level of sophistication. Hence, only commodity hardware are used.

In this paper, we consider the following three attack scenarios. Although more scenarios are possible, the scenarios below have in common that attacks can be mounted while the target vehicle is driving at high speed, as opposed to low-speed activities such as parking. The motives for the attacks are to either cause as much damage as possible, such as provoking a car accident, or to force a car into its minimal risk condition (i.e. stopping safely on the shoulder lane [32]), or to simply disrupt road traffic.

Front/rear/side attack In a front/rear/side attack, the attacker installs the required hardware to mount an attack in another vehicle. Depending on the hardware, this can be installed without anyone noticing. The vehicle is then used to drive in front of (or behind of, or next to) the target vehicle. When positioned, the attack is executed once or multiple times. The advantage of this attack scenario is that it allows an attacker to keep the same distance to the target AV for a longer period.

Roadside attack A roadside attack is mounted stationary in objects on the side of the road, such as the guard rail. The attack is not limited to one installation point, but can be spread over multiple installation points, potentially connected to each other (e.g. for replay or relay attacks).

Evil mechanic attack The 'Evil Mechanic' [28] has short-term physical access to the vehicle, e.g. when it is parked or left for maintenance. For instance, an attacker can mount a jamming device on a (carrier) vehicle that jams other vehicles unknowingly.

The devices-under-test are considered black-boxes, of which the hardware layer is attacked. Even though the technical specifications and datasheets are available, the exact internal workings are not documented. No internal signals will be used and no detailed information on the hardware is assumed to be known. With respect to the attacker model, this is a valid assumption. Because of the limited money and limited time, the attacker cannot reverse engineer all existing systems, and can only apply general techniques. The attacker is aware of what the hardware is supposed to do, but is not aware of how it works internally.

5. ATTACKS ON CAMERA

A camera can be used to detect traffic signs, delineation, or objects, it can be attacked in multiple ways. Detection of traffic signs can be fooled by placing (fake) traffic signs at improper locations. It is also possible to 'hide' traffic signs by surrounding them with other shapes/colors to confuse shape/color detection algorithms [11]. Lane detection can be confused by painting additional lines on the road, or by using different colors (this is already the case at road construction sites). Object tracking is usually limited because of computational power or resolution, so it would be easy to cause a denial of service by presenting too many objects to track. Recently, it has been demonstrated that deep neural networks (DNNs) (which achieve state-of-the-art performance on visual classification problems, and are used in camera software) can be easily fooled by completely unrecognizable images to humans, but that DNNs believe to be recognizable objects with 99.99% confidence [26].

Attacks on camera can also target its features such as automatic exposure controls, auto-focus or light sensitivity. Indeed, cameras normalize lighting conditions via an iterative process. When light is directed at the image sensor, it will tune down its sensitivity and exposure to improve the image quality according to predefined settings. This can lead to undesired effects, for instance when the auto exposure tunes down due to headlights at night. This could hide information in the background, such as traffic signs, road edges or pedestrians. The Google Driverless Car is susceptible to this problem [8].

In Sections 5.1 and 5.2, we demonstrate attacks that aim to hide objects and fool auto-controls. The attacker will use commodity hardware such as a laser pointer or cheap LEDs. To assess the effectiveness of the attack we use the tonal distribution, which represents the distribution of the number of pixels per grayscale value, with a total of 256 bins. All images presented here are 320 x 240 pixels, and all tonal distributions have the same domain and range.

5.1 Blinding the camera

The goal of this attack is to blind the camera fully or partially, by emitting light into the camera in order to hide objects. Failing to detect objects such as speed limit signage or traffic light can jeopardize passenger's safety.

5.1.1 Description

Blinding occurs when the camera is not able to tune the auto exposure or gain down anymore. In this case, the light cannot be dimmed, which results in an overexposed image. Three variables have direct impact on the effectiveness of the blinding attack. The first variable is the environmental light. If the camera is positioned in a bright environment, the auto controls are adapted for that particular environment, so more light would be needed to raise above the environmental light to reach a blind state. The second variable is the light source used to blind (i.e. wavelength), and the third variable is the distance between the light source and the camera. Therefore, experiments were done in bright (250 lx) and dark (0 lx) environments, with different light sources at multiple distances (50 cm, 100 cm, 150 cm and 200cm). One should note that increasing the distance would require to increase the number of light sources. The amount of light sources can be approximated with the 'Inverse-square Law', which shows that the number of light sources required to have the same power grows exponentially with the distance.

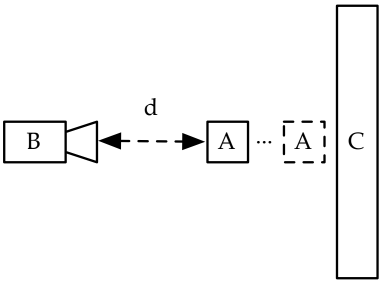
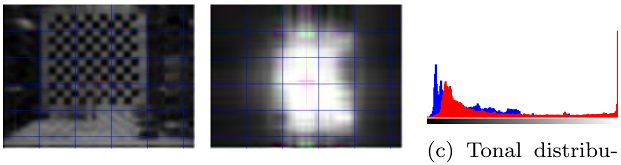


Figure 3: Setup of blinding experiment



(a) Laser off

(b) Laser on

(c) Tonal distribution

Figure 4: Blinding MobilEye C2-270 with 650 nm laser

The results from a near-infrared sensitivity test (left out here for space reason) show that Ledsee 650 nm diode point laser is the most effective, followed by the Osram SFH4550 IR 850 nm LED and the Ledsee IR 940 nm 5x5 LED matrix. Figure 3 depicts the experimental setup of the blinding attack, where B is the camera, A the light source (positioned at different distances) and C the background (a checkerboard pattern).

5.1.2 Results

For space reason, only results from the most effective light source are discussed here[1]. Figure 4 shows the result of blinding by 650 nm laser. In Figure 4a the laser is off and the camera sees the background. In Figure 4b, the laser is on and the background is not visible anymore, causing a partial blinding. Indeed, Figure 4c shows a clear shift in tonal distribution, as denoted by the red peak on the right (blue corresponds to the off-state, red to the on-state).

Table 1 presents the correlation between the off-state and on-state tonal distributions per light source. A high correlation value indicates more similarity between two images. Therefore, lower values are more interesting because indicate change in lighting condition, and thus, potential blinding. The correlation values between 0%-50% and 0%-100% power are presented to see if the amount of power influences

[1] All results are available here: https://mega.nz/#F!DMglBZ4J!yNEq99B-kvYeUK_Rhb7dtA

the result.

Light source	Visible	Setting	Distance	CV1	CV2
365 nm LED spot	yes	dark	50 cm	0.437	**0.084**
365 nm LED spot	yes	dark	100 cm	0.860	0.524
365 nm LED spot	yes	dark	150 cm	0.993	0.858
365 nm LED spot	yes	dark	200 cm	0.691	0.758
365 nm LED spot	yes	light	50 cm	0.992	0.985
365 nm LED spot	yes	light	100 cm	0.999	0.998
365 nm LED spot	yes	light	150 cm	0.999	0.998
365 nm LED spot	yes	light	200 cm	0.998	0.996
White LED spot	yes	dark	50 cm	**0.098**	0.109
White LED spot	yes	dark	100 cm	**0.120**	0.118
White LED spot	yes	dark	150 cm	0.280	0.230
White LED spot	yes	dark	200 cm	0.748	0.323
White LED spot	yes	light	50 cm	0.492	0.400
White LED spot	yes	light	100 cm	0.901	0.777
White LED spot	yes	light	150 cm	0.946	0.941
White LED spot	yes	light	200 cm	0.924	0.927
850 nm LED spot	no	dark	50 cm	0.173	0.165
850 nm LED spot	no	dark	100 cm	0.716	0.779
850 nm LED spot	no	dark	150 cm	0.966	0.796
850 nm LED spot	no	dark	200 cm	0.971	0.911
850 nm LED spot	no	light	50 cm	0.989	0.977
850 nm LED spot	no	light	100 cm	0.996	0.997
850 nm LED spot	no	light	150 cm	0.997	0.996
850 nm LED spot	no	light	200 cm	0.996	0.997
940 nm 5x5 LED matrix	no	dark	50 cm	**0.161**	0.613
940 nm 5x5 LED matrix	no	dark	100 cm	0.727	0.096
940 nm 5x5 LED matrix	no	dark	150 cm	0.970	**0.086**
940 nm 5x5 LED matrix	no	dark	200 cm	0.994	**0.069**
940 nm 5x5 LED matrix	no	light	50 cm	0.985	0.832
940 nm 5x5 LED matrix	no	light	100 cm	0.998	0.951
940 nm 5x5 LED matrix	no	light	150 cm	0.994	0.969
940 nm 5x5 LED matrix	no	light	200 cm	0.999	0.986
650 nm laser	yes	n/a	n/a	n/a	**0.152**

Table 1: Correlation between 0%-50% (CV1) and 0%-100% (CV2) power observations. Lower correlation values indicate less similarity between observations. Lower is better.

The results show that the correlation value increases with the distance, which was expected as less light reach the camera sensor at larger distances. The environmental light has influence on the results, as the correlation values in light conditions are all in the range of 0.95 - 1.0, except for the white LED spot. So, in light conditions, the most effective light sources are the 650 nm laser and the White LED spot. One should note that for the 650 nm laser, *n/a* means that environmental light, distance and power do not influence the blinding effectiveness. In dark conditions, the IR 940 nm 5x5 LED Matrix has the most influence (and is the cheapest of all the light sources used in this experiment), followed by the White LED spot.

Although this experiment did not succeed to fully blind the image using near-infrared light sources, these light sources can be used to blind objects. For instance, by mounting several LEDs on a vehicle that should normally be recognized, the MobilEye C2-270 cannot recognize them anymore. In general, blinding a camera will work best from a front/rear/side attack, since the light sources should be positioned carefully to emit the most light into the image sensor (see Section 7).

5.2 Confusing the auto controls

Compared to the blinding attack that aims to max-out the camera auto controls, this experiment focuses on influencing the auto controls in the period before the image recovers and stabilizes. Hence, this attack is harder to detect by the system because consists of burst of light instead of a constant beam. The longer it takes to stabilize to the new environmental conditions, the longer the car is vulnerable to objects it cannot detect. This attack distinguishes itself from situations like driving out of a tunnel, because in that case, the camera can adapt more gradually to the new conditions. Confusing the auto controls is limited to front/rear/side attack, because it assumes that the attacker continuously switches the light on and off.

5.2.1 Description

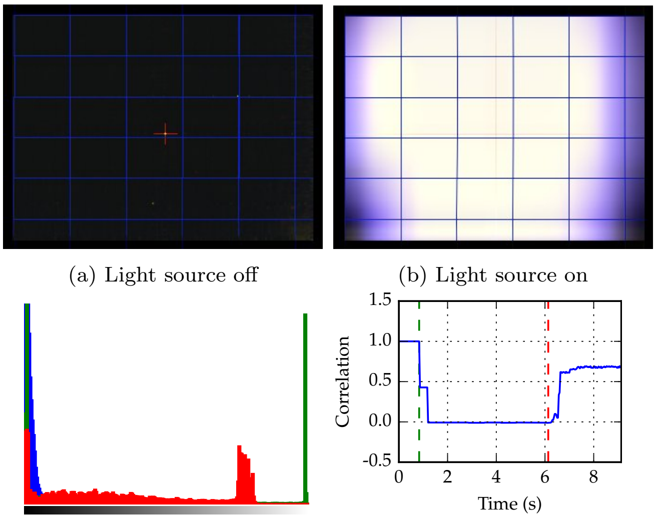
The MobilEye C2-270 camera sensor is equipped with auto exposure control and auto gain control. It is undocumented if both auto controls are enabled, but for optimal image quality in darker environments, it is presumed to be the case. Auto exposure control will determine the shutter speed for each frame, while auto gain control can amplify the electron charges from the image sensor after exposing it to the light. Both controls measure the current scene luminosity and desired output luminosity by accumulating a histogram of pixel values. This value is then used to calculate the desired exposure and gain values. Both controls need some time before being stable, because of their iterative control process. On the other hand, having a too fast loop control would make the image very unstable in terms of brightness.

The experimental setup is the same as for the blinding attack, but with a black curtain as background to make sure the MobilEye C2-270 is as sensitive to the light source as possible. All of the light sources of the previous experiment were tested. For each test, a video was recorded. Each test starts in a 'starting condition'. Then, the light source is turned on to full power in one shot, and the video is stopped when the camera has adapted to the new light source. To analyze each video, a tonal distribution is created for each frame, after which, each consecutive tonal distribution is correlated with the first one (the 'starting condition'). The time between the first drop in correlation, and the first rise (if applicable) is measured, and denotes the vulnerable period (e.g. blinding time).

5.2.2 Results

For space reason, only results from the most effective light source are discussed here[2]. Figure 5 shows the result of the experiment with the 940 nm 5x5 LED matrix in dark environment at 50 cm. Figure 5a shows the initial state of the camera facing the LED matrix (off). When the LED matrix is turned on (Figure 5b), the image is almost fully blinded. This is confirmed by Figure 5c, in which the two peaks on the right (the green (resp. red) corresponds to 50% power (resp. 100%)) demonstrate that the light source affects the amount of black tones in the image. Figure 5d shows the time to recover from the attack. The left vertical dashed line (green) represents when the LED matrix was turned on. We can see a drop in correlation from 1 to -0.012. The right vertical dashed line (red) represents when the LED matrix was turned off. During the attack window (1 to 6 seconds) the correlation drops to zero. When the LED matrix is turned off, the camera recovers to a normal state in 0.3 second. In total, the 940 nm 5x5 LED matrix blinded the camera for 5.3 seconds.

[2] All results are available here: `https://mega.nz/#F!DMglBZ4J!yNEq99B-kvYeUK_Rhb7dtA`



(a) Light source off

(b) Light source on

(c) Tonal distribution

(d) Time to recover

Figure 5: Auto-Exposure MobilEye C2-270 with 940 nm 5x5 LED matrix

Light source	Visible	Setting	Distance	Blinding Time	MCV
365 nm LED spot	yes	dark	50 cm	0.67	0.201
365 nm LED spot	yes	dark	100 cm	0.63	0.706
365 nm LED spot	yes	dark	150 cm	—	0.969
365 nm LED spot	yes	dark	200 cm	—	0.981
365 nm LED spot	yes	light	50 cm	0.97	0.504
365 nm LED spot	yes	light	100 cm	—	0.921
365 nm LED spot	yes	light	150 cm	—	0.945
365 nm LED spot	yes	light	200 cm	—	0.939
White LED spot	yes	dark	50 cm	1.67	0.116
White LED spot	yes	dark	100 cm	1.33	0.409
White LED spot	yes	dark	150 cm	0.43	0.470
White LED spot	yes	dark	200 cm	0.77	0.551
White LED spot	yes	light	50 cm	0.37	0.076
White LED spot	yes	light	100 cm	0.40	0.079
White LED spot	yes	light	150 cm	0.73	0.367
White LED spot	yes	light	200 cm	0.37	0.474
650 nm laser	yes	n/a	50 cm	∞	-0.100
650 nm laser	yes	n/a	100 cm	∞	-0.011
850 nm LED spot	no	dark	50 cm	4.67	-0.017
850 nm LED spot	no	dark	100 cm	2.97	-0.001
850 nm LED spot	no	dark	150 cm	—	-0.035
850 nm LED spot	no	dark	200 cm	4.30	-0.064
850 nm LED spot	no	light	50 cm	5.50	-0.033
850 nm LED spot	no	light	100 cm	1.67	-0.021
850 nm LED spot	no	light	150 cm	2.67	0.0267
850 nm LED spot	no	light	200 cm	5.00	0.1229
940 nm 5x5 LED matrix	no	dark	50 cm	5.30	-0.012
940 nm 5x5 LED matrix	no	dark	100 cm	5.47	-0.014
940 nm 5x5 LED matrix	no	dark	150 cm	1.67	-0.017
940 nm 5x5 LED matrix	no	dark	200 cm	4.67	-0.017
940 nm 5x5 LED matrix	no	light	50 cm	**6.00**	-0.016
940 nm 5x5 LED matrix	no	light	100 cm	3.17	-0.041
940 nm 5x5 LED matrix	no	light	150 cm	4.33	-0.022
940 nm 5x5 LED matrix	no	light	200 cm	1.33	-0.027

Table 2: Blinding times (in seconds) and the minimal correlation values (MCV).

The results of all light sources tested are presented in Table 2. The correlation score is the lowest score calculated over all frames. A high value indicates more similarity between two images, whereas a low value indicates less similarity. Therefore, lower values are more interesting, and indicate how much the image was blinded.

Compared to results of Section 5.1, the environmental light has less influence on the outcome of the attack. Indeed, blinding time and MCV are similar in dark and light conditions. Likewise distance does not affect significantly the attack. Results for the 650 nm laser show that the camera does not recover from the intense beam, therefore the blinding time is infinity. The 940 nm 5x5 LED matrix and 850 nm LED spot are also very effective and provide blinding times greater than 5 seconds and low correlation values. This attack demonstrates that MobilEye C2-270 auto controls can be confused, and that in some case the camera never recovers from it.

5.3 Countermeasures

Countermeasures exist to protect cameras from being tampered with. There is a trade-off between protecting the camera from tampering, sensitivity, image quality, camera size and price. Most of the countermeasures require the camera to be modified. This not only increases the cost, but also the dimensions of the device, which can be problematic for the cost-driven and space-restricted automotive environment.

5.3.1 Redundancy

By introducing multiple cameras that perceive the same image (or at least overlap), the attacker has to put more effort into the attack to blind all cameras at the same time. Experiments have shown that using a 650 nm laser (5 mW) is the most effective way to temporary blind a camera. Unfortunately, due to the small beam width, this attack is only limited to a single image sensor at a time. At a distance of 50 cm, the width of a focused beam was measured at approximately 1.5 mm. The size of the MobilEye C2-270 lens was measured at approximately 5 mm. Introducing extra cameras may not protect from military grade weapons such as a 'Dazzler' [1]. Indeed, the width of the Dazzler's beam can be configured up to 12 cm, at the expense of output power on the same area and range. This makes it a lot easier for an adversary to aim at a camera sensor. If multiple cameras are used to complement each other, then it is also possible that the 'Dazzler' will hit several camera sensors at the same time.

However, redundancy requires more space to fit the cameras and cameras need to be carefully calibrated so the overlapping image is not misaligned. Software should blend the separate images together, which is rather trivial as long as cameras have a static position with respect to each other. Other challenges of this countermeasure include synchronized capturing and maintaining the same exposure [2].

5.3.2 Optics and materials

Integrating a removable near-infrared-cut filter, a technique that is available on security cameras, can filter near-infrared light on request. The filter can be applied by switching an electromagnet. During day time, the filter is applied to yield a better image. During night time the filter is removed to make use of infrared light for night vision. When the filter is applied, it will also block infrared light sources, hence this countermeasure is only effective during day time.

To improve this countermeasure, the filter could also be applied when the camera decides it is needed, for instance when it is jammed (see next countermeasure), or when the auto controls cannot be optimized for the bright lighting conditions anymore. In this case, it is assumed that jamming the sensor is already in progress. This may introduce a new attack vector, as an attacker may repeatedly attack the auto controls (as demonstrated in Section 5.2) to let the camera apply the filter or remove it. Depending on the quality of the near-infrared-cut filter, the camera may thus be damaged.

Another option is to use photochromic lenses. These types of lenses can change color to filter out specific types of light. An example includes glasses with darkening lenses in sunlight. The type of lenses (or coating on the lenses) determine the type of light it filter. For example, vanadium-doped zinc telluride is a material that can filter light with a wavelength of 630 nm - 1300 nm [38]. High-intensity beams will make the material more opaque, therefore filter more. The advantage of these type of materials is that they do not affect the image in low-light conditions.

6. ATTACKS ON LIDAR

Since LiDAR is the preferred technique in speed measurement devices, jammers are widely available on the (black) market. However, a LiDAR can only see things that are reflected by the signal. If the signal does not return (due to absorption, transparent objects or range limits), it will assume there is 'nothing'. For a 360° view, most of the world will be classified as 'nothing'.

Reflective objects can confuse a laser beam as reflected objects can appear in the field-of-vision while they should not, which is major problem for Collision Avoidance Systems. For instance, objects located behind can be detected as in front. Also, some objects on the road are reflective by design. Lane markings reflect some of the signal, so it will be visible in the perceived image.

Because LiDAR plays a major role in automated vehicle's perception and simply uses light pulses, it is an obvious attack surface. The main goal of attack on LiDAR is to generate noise, fake echoes, or fake objects. In this Section, we assess the feasibility and sophistication of attacks on LiDAR. We performed replay, relay, jamming and spoofing attacks on LiDAR, which were all successful. However, for space reason and because they are respectively an extension of replay and jamming attacks, only the relay and the spoofing attacks are presented in this paper[3].

6.1 Relaying the signal

This attack is an extension of replay attack that aims at relaying the original signal sent from the target vehicle LiDAR from another position to create fake echoes, and eventually, make real objects appear closer or further than their actual locations.

6.1.1 Description

To perform the relay attack, an attacker needs two transceivers (B and C in Figure 6). As the ibeo LUX 3 uses light with a wavelength of 905 nm, transceiver B is a photodetector sensitive to this wavelength (Osram SFH-213, costing 0.65 US$). The output of B is a voltage signal that corresponds to the intensity of the pulse sent by the LiDAR (A). An oscilloscope is attached to B to visualize the signal. The output of B is sent to C, which uses a laser (Osram SPL-PL90, costing 43.25 US$) to emit a pulse in return.

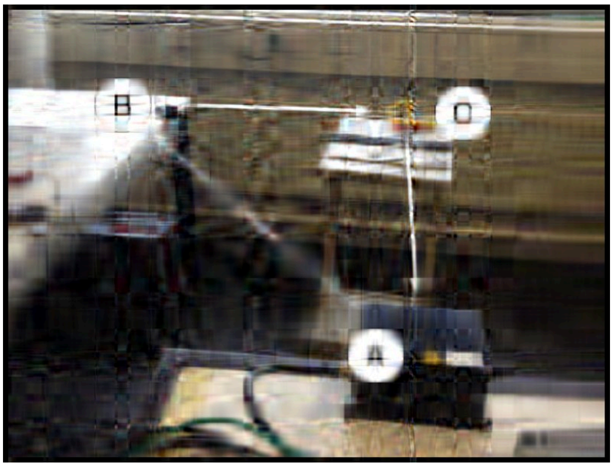


Figure 6: Setup of a LiDAR relay attack

In Figure 6, both transceivers are positioned one meter away from each other, but they do not have to be at the same physical position for a relay attack. The relay attack also performs well if the transceivers are positioned behind the ibeo LUX 3. Indeed, since the LiDAR signals reflect, some of the reflected light that travels back will also travel past the ibeo LUX 3. If a transceiver receives it over there, the same signals can be retransmitted from another location. Therefore, a direct line of sight is not required to perform a relay attack with these transceivers. A relay attack is most likely to happen from the roadside, where an attacker would receive LiDAR signals from vehicles and relay them to another vehicle located at a different location.

6.1.2 Results

Figure 7 shows the impact of the relay attack on the LiDAR perception. Before the attack, the LiDAR only detects the wall located at one meter in front of it (represented by the small yellow horizontal line at the center of the bottom of Figure 7). During the relay attack, the LiDAR receives echoes from objects at 20 and 50 meters away (circled in Figure 7). Because the automation system detects obstacles further away, these echoes can affect the mission planning (see Section 7.4 for detailed discussion). This attack shows that pulses are not encoded for the LiDAR that emits them, and that pulses can be replayed and relayed to generate fake echoes.

6.2 Spoofing the signal

The relay attack demonstrated that fake echoes can be easily injected. In this Section, we extend the attack by creating fake objects. This experiment will use the original signal as a trigger point to actively spoof the ibeo LUX 3, with the intention to re(p)lay objects and control their position.

6.2.1 Description

Light travels with a speed of approximately $3 \cdot 10^5$ km/s, or 1 meter every 3.33 ns. With a maximum range of 200 meters

[3] Results and videos of attacks are available here: `https://mega.nz/#F!DMglBZ4J!yNEq99B-kvYeUK_Rhb7dtA`

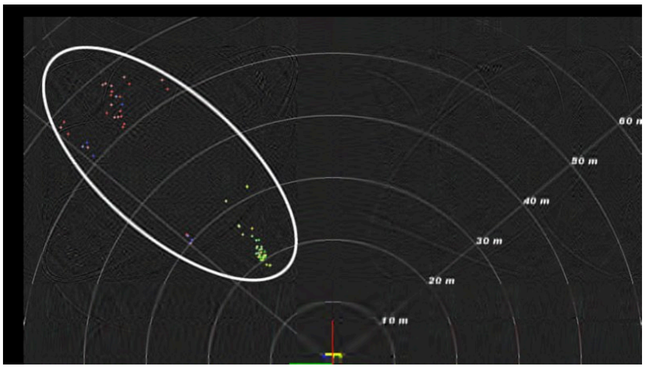


Figure 7: Result of LiDAR relay attack. Light pulses are received from the left, and relayed from the right.

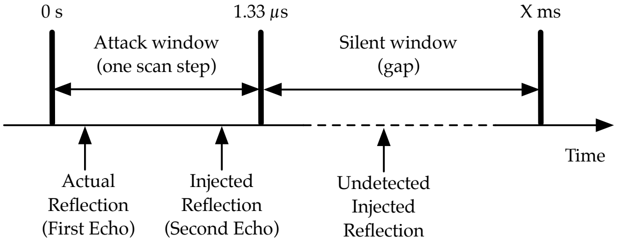
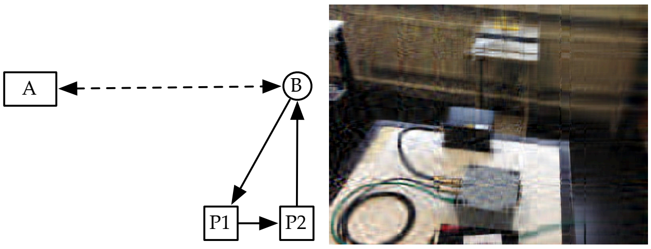


Figure 8: LiDAR attack window. The arrows indicate what would happen if the attacker's pulse hits the LiDAR at that time.

for the ibeo LUX 3, the signal travels this distance back and forth in approximately 1.33 μs. This means that the LiDAR should listen for at least 1.33 μs for incoming reflections. To successfully inject signals into the LiDAR, the counterfeit signal should arrive within this window. The earlier the LiDAR receives the signal, the closer it will be to the LiDAR. Therefore, if the attacker delays the original signal before it relays it, it can control the position of the objects. Do note that if, for instance, the attacker is at 200 meters, the attack window is smaller since the first 200 meters have already been travelled by the light pulses.

Figure 8 relates timing to the success of spoofing attacks. In the attack demonstrated here, the counterfeit pulse is received by the LiDAR after the first echo is received (the original pulse). This makes a point appear further away, as the LiDAR thinks it travelled a longer distance. If the counterfeit pulse is received in the silent window (gap), i.e. after the 1.33 μs attack window, it will not be noticed. This is why the attacker needs to know when to generate pulses.

Figure 9 depicts the experimental setup. The ibeo LUX 3 is represented by A, the transceiver by B and the control logic by P1 and P2 (not shown in actual setup). A counterfeit signal is generated via external control logic, consisting of two pulse generators. The output of B is connected to the trigger input of the HP 8011A pulse generator (P1). As soon as P1 is triggered, it will delay the output. The output of P1 is connected to the input of the second pulse generator, a Philips PM 5715 (P2). A fixed number of square-wave pulses can be generated as soon as P2 is triggered. The output of P2 is then sent back to the transceiver. In this experiment, the attacker aims at injecting copies of the real wall located at one meter, and this, at different distances.



(a) Schematic (b) Actual setup

Figure 9: Setup of a LiDAR spoofing attack

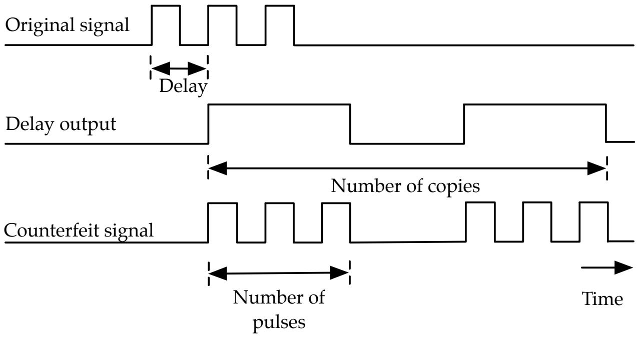


Figure 10: The delay, number of copies and number of pulses are the parameters used to create counterfeit signal.

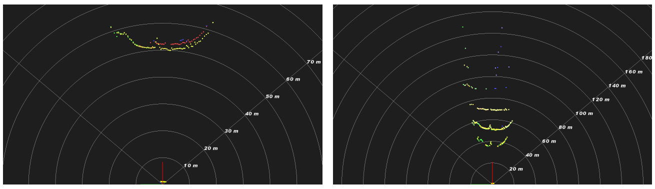
The delay, number of pulses, number of copies, pulse width and pulse period are the variables that can be controlled. Figure 10 shows how the trigger delay and the number of copies affect the counterfeit signal. As soon as one pulse triggers the control logic, a similar signal is generated of a fixed number of pulses. By tuning the pulse width and pulse period using an oscilloscope, the counterfeit signal can resemble the original one.

6.2.2 Results

Figure 11 shows the result of the spoofing attack on the LiDAR representation. Figure 11a shows points that resemble a copy of the wall detected at approximately 50 meters. The LiDAR considers these points at second echoes. By tuning the delay, it is possible to make the wall appear closer or further away, until the signal falls outside of the attack window.

P1 can be configured to output multiple pulses when it is triggered. Therefore, it is possible to inject multiple counterfeit pulses in a sequence. Figure 11b shows the result of the spoofing attack, where multiple copies of the wall were generated at regular spaced intervals. These fake walls are detected at 40, 50 and 70 meters away from the LiDAR. The first copy of the wall is considered as second echoes, the others are a mix of second and third echoes, until it fades out.

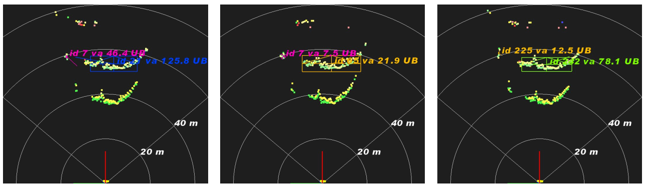
As mentioned earlier, the ibeo LUX 3 can classify and track objects. When the "tracking box" is connected to the Li-



(a) spoofing of one copy of the wall

(b) spoofing of multiple copies of the wall

Figure 11: Results of a LiDAR spoofing attack



(a) $t = 10.37$ sec, $ID = 21$

(b) $t = 10.59$ sec, $ID = 65$

(c) $t = 10.83$ sec, $ID = 242$

Figure 12: Tracking the second wall over time. A new color represents a new object. For clarity, the tracking boxes for the other objects are not shown.

DAR, the ibeo LUX 3 allocates object numbers to detected objects. We re-run the same experiment as in Figure 11b with tracking enabled. The ibeo LUX 3 classified the walls as 'Unknown big' (and sometimes even as 'Car'). Figure 12 shows three consecutive snapshot of the LiDAR representation. We can see that the second counterfeit wall is detected and classified as 'Unknown big' (UB) and that its object number changed. In less than 0.46 second, the second wall is identified as three new objects. This indicates that the ibeo LUX 3 classifies the same spoofed object as a new object, therefore is unable to track an object over time. This attack proves that fake objects can be spoofed, classified and (tentatively) tracked by the LiDAR.

6.3 Countermeasures

The countermeasures below can be implemented in software (except redundancy) to prevent or detect the attacks demonstrated in this paper. A modification of the sensor hardware is not necessary, but the firmware can be changed to implement some of the countermeasures proposed (at the expense of range or accuracy). However, no information can be provided to indicate if the countermeasures are already implemented in the object tracking software of ibeo LUX 3, as the sensor was only tested on raw data level.

6.3.1 Redundancy

The experiments have shown that it is possible to relay and spoof on the ibeo LUX 3. According to [21, 33], it is possible to use different types of wavelengths for LiDAR vision[4]. Although some wavelengths have drawbacks in terms of range, combining multiple wavelength LiDAR makes it harder for the attacker to attack both signals at the same time. According to [33], the costs for the required hardware will exceed the budget for the attacker model considered in this paper.

Another way of adding redundancy would be to use V2V communication[5]. If an attacker mounts a front/side/rear or roadside attack, it is likely to only affect a single vehicle. If other AVs share their measurements, the attacked AV could compare its measurements with what other vehicles observe in order to detect inconsistencies. This countermeasure opens up new attack surfaces as neighboring vehicles may intentionally share incorrect data.

6.3.2 Random probing

As shown in Section 3.2, the pulse is repeated at a fixed interval. This interval depends on the scanning speed, and thus, the rotation of the mirror inside the ibeo LUX 3. Furthermore, the attacker needs to synchronize on this interval, so it knows exactly when to fire a pulse back. By varying this period non-predictably, it will be harder for the attacker to synchronize on the original signal. This countermeasure can be problematic for rotating LiDAR because they require a constant rotation speed and need to know exactly at which angle they fired a pulse.

Another option is to (non-)predictably skip certain pulses. This countermeasure only requires a modification of the software that controls the laser emission. When a pulse is skipped, it introduces an effect that is similar to varying the scan speed. If the LiDAR skips a pulse, it can still listen for incoming pulses. If it notices a response, this may indicate that an attack is going on. It depends on the application whether this is acceptable or not. However, at a scan frequency of 50Hz, missing a few pulses will not have much effect on the resolution, especially at close range.

6.3.3 Probe multiple times

This countermeasure is only effective against random jamming. If an attacker is not in sync with the pulse signal generated by the LiDAR, counterfeit pulses will appear at random intervals in the attack window. For instance, if the LiDAR measures three times at a the same position and it measures three different distances (e.g. 40 m, 10 m, 150 m), this measurement is likely to be invalid.

Probing multiple times does introduce three new problems. First, it decreases the scan frequency. Probing four times will effectively convert a 50Hz device LiDAR into a 12.5Hz device. Second, the measurements should be corrected, to compensate for any movement of the vehicle in between the measurements. This should not be a major limitation, since most modern vehicles advertise the speed of the vehicle via the CAN bus. Lastly, the software should detect invalid measurements. Removing outliers will have a small impact on resolution, but at close range, this may not be a problem. Another option can be to average the measurements using a rolling average or Kalman Filter. This countermeasure can be implemented in software.

6.3.4 Shorten the pulse period

In Section 6.2 it was calculated that the ping period is approximately 1.33 μs. This gives the attacker an attack win-

[4] Do note that the wavelengths should not overlap. However, using a 850 nm LiDAR will still influence the 905 nm LiDAR.

[5] This countermeasure will also work for camera-based system.

dow of less than 1.33 μs. By shortening the pulse period, we reduce the attack window. One should note that lowering the pulse period will also lower the maximum range. By halving the period to 0.66 μs, the range of the ibeo LUX 3 will decrease to 100 meters.

The effectiveness of this countermeasure depends on the type of attack. For instance, in a front/rear/side attack, this countermeasure is less effective, as the attacker is allowed to constantly move around the target vehicle (e.g. have a jammer installed in the bumper and drive in front of the target). For a roadside attack, this countermeasure is more effective because the maximum range decreases.

7. DISCUSSION

In this Section we discuss the limitations of the attacks presented in this paper and their impact on the application layer.

7.1 Limitation 1: Generating Closer Objects

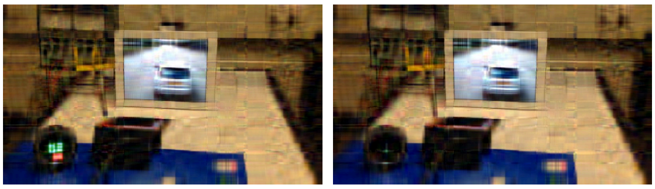
The relay attack in Section 6.1 directly connected the output of one transceiver to the input of the other. Even if no additional delay was introduced, the closest we could inject fake objects was at 20 meters from the LiDAR, while the original object was located at 1 meter. Experiments of Section 6.2 suffer from the same issue. For instance, in Figure 11b it was only possible to inject a copy of the wall at approximately 40 meters. At low speed, an AV (or even a human) would have enough time to react. However, at high speed this is major problem as it takes approximately one seconds to travel 40 meters, leaving almost no time to brake or maneuver. We noticed that cable length and transceiver circuits caused an intrinsic delay of 64 ns, corresponding to the 20 meters.

7.2 Limitation 2: Attack Range

Regarding the LiDAR experiments, no range tests have been performed. The laser part of the transceiver has a range up to 100 meters with a viewing angle of 9°. Therefore, it will be easy for an attacker to emit a laser beam at a large distance on a moving vehicle, which is the only part required for a jamming attack. But for relay, and in particular spoofing attacks, receiving the original signal is more important. Larger distances between the attacker and its target will increase the gap between LiDAR pulses. At a distance of 100 meters, the gap between two sequential LiDAR pulses is approximately 1.47 meters. Since a photodetector has an aperture of only 5 mm, it is very likely that pulses will not be detected. Thus, multiple photodetectors will be required, increasing the cost of the attack. Moreover, as explained in Section 6.2, the distance between the attacker and its target directly impact the attack window. So, the attacker might not have an interest in being too far from the target AV.

7.3 Limitation 3: Indoor Experiments

All attacks presented here were performed in laboratory conditions. Performing such attacks outdoor, on moving vehicles, is more challenging and might require additional hardware. The main issue of attacking camera is *aim*. Indeed, the attacker has to accurately target the camera sensor, which can be challenging in moving condition (front/rear/side or roadside). For example, the 650 nm laser (which has the most influence on the MobilEye C2-270) has a beam of 1.5 mm that makes aiming very challenging for human. Therefore, an attacker could use an Arduino object tracking device that can follow object at high speed. For the LiDAR the main issue is *synchronization to the pulse period*. Especially, this has to be done quickly when the attack is performed from the roadside. However, we would like to stress that indoor experiments do not lessen the validity of our experimental results. We expect similar results in outdoor experiments.


(a) Laser off, normal behavior of MobilEye C2-270

(b) Laser on, MobilEye C2-270 does not detect vehicle ahead

Figure 13: MobilEye live blinding experiment.

7.4 Impact on Application Layer

The attacks demonstrated in this paper are directed at the hardware layer (i.e. 'Sense' or *raw data level*) and demonstrated that the ibeo LUX 3 and the MobilEye C2-270 did not detect malicious input. This may be completely different for other systems and implementations available on the market, but it is believed that fully automated vehicles that currently exist will also fail to detect malicious input. Therefore, we go beyond the hardware layer and discuss the impact of the attacks on the application layer (i.e. 'Understand' and 'Act' in Figure 1). The application layer involves sensor processing, sensor fusion and decision upon driving actions. The processing steps for the MobilEye C2-270 and the ibeo LUX 3 are not documented. However, it is interesting to see how the application layer processes malicious input and if it can detect it.

In the first experiment, an iPad is put in front of the MobilEye C2-270 camera. The objective is to show that the CAS fails to work when the camera is blinded. The MobilEye C2-270 is connected to a simulator that is setup to report a speed of 130 km/h[6]. A video is played with footage from a dashboard camera, as if the MobilEye C2-270 was installed in an actual vehicle. First, Figure 13a shows what would happen without any tampering, then the laser pointer is turned on, with the intention to blind the camera. Figure 13b shows that the display is blank, meaning that the vehicle ahead is not detected.

The ibeo LUX 3 contains an embedded tracking system. The tracking system can group points and classify them as a car, truck, bike, pedestrian or unidentified object. It can also track objects over time. This allows the ibeo LUX 3 to determine an object's direction. Section 6 demonstrated that the LiDAR is sensitive to counterfeit pulses generated by an adversary. Furthermore, it was possible to control the distance where objects appeared, by varying the delay of the trigger signal of the second pulse generator. Figure 14 shows

[6] At least 40 km/h is needed to trigger collision warnings.

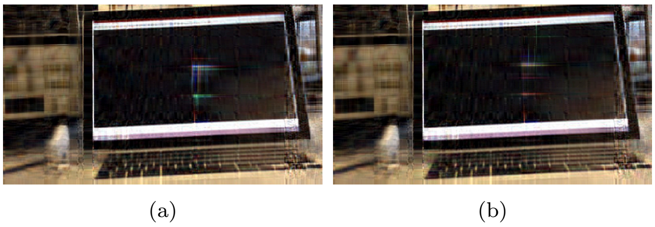

(a) (b)

Figure 14: ibeo LUX 3 live experiment. The objects change direction (the lines), as instructed by the attacker.

two sequential frames of the LiDAR, and shows how the position of the objects reverses immediately. While this is not problematic for the tracking software, it can potentially confuse the decision system of an AV. Furthermore, there is a limit on the number of objects that can be tracked by the ibeo LUX 3. By introducing noise or more sophisticated objects, a denial-of-service attack can be mounted on the LiDAR, by introducing a large number of noise or spoofed objects. The ibeo LUX 3 would then track fake objects while real objects wouldn't be detected anymore.

Based on this object detection, the automation system will adapt its short-term planning (e.g. preparation of maneuvre to avoid obstacle) or mid-term planning (e.g. modification of the route to react to road block ahead). Therefore, the attacker does not necessarily need to inject fake objects close to the target vehicle to impact its driving behavior. However, checking how automation system reacts to malicious sensor data would require access to the complete vehicle automation system, which is part of our future work. One should note that the current work used raw data level and that typical sensor system output to the OBU at an object level and performs some sort of data sanitisation.

8. CONCLUSIONS AND FUTURE WORK

Automated vehicles are becoming a reality and car manufacturers foresee deployment in a near future. Autonomous automated vehicles unconditionally rely on their on-board sensors to detect surroundings objects and understand their environment. Valid and accurate sensor data are required to make appropriate driving decisions such as emergency brake, changing trajectory or rerouting. In this paper we demonstrated remote attacks on two perception systems: camera (MobilEye C2-270) and LiDAR (ibeo LUX 3). By performing attacks with commodity hardware, we proved their feasibility and effectiveness. Specifically, we shown blinding and confusing auto controls attacks on the camera, and relaying and spoofing attacks on the LiDAR. For the MobilEye C2-270, a simple laser pointer was sufficient to blind the camera and prevent detection of vehicle ahead. A cheap transceiver was able to inject fake objects that are successfully detected and tracked by the ibeo LUX 3. These attacks prove that additional techniques are needed to make the sensor more robust to ensure appropriate sensor data quality. Thus, we proposed countermeasures to mitigate these attacks. As the automotive domain is strongly cost-driven, the proposed countermeasures are mostly applicable in software. Finally, we discussed limitations of our experiments and potential impact on the application layer.

Our future work are fourfold. First we will reproduce the attacks outdoor in moving vehicles. Secondly, we will get access to the full automation system to investigate the impact of attacks on the driving decisions. We will extend the experiments by attacking multiple sensors at the same time to stress even more the system and check its reaction. Thirdly, we will get access to other models of sensors to generalize the applicability of our attacks. Finally, we will implement the proposed countermeasures to validate them.

9. ACKNOWLEDGMENTS

We would like to thank V-TRON and IBEO for supporting this research by giving access to the equipments.

References

[1] Armaser. Laser Dazzlers. `http://www.armlaser.com/laser-dazzlers-c-30.html`. Accessed: 2015-05-12.

[2] C. Arora, S. Singla, S. Singh, and A. Gupta. Seam Reconstruct: Dynamic scene stitching with Large exposure difference. In *2nd International Conference on theApplications of Digital Information and Web Technologies (ICADIWT)*, pages 574–578, 2009.

[3] L. Bai and Y. Wang. A Sensor Fusion Framework Using Multiple Particle Filters for Video-Based Navigation. *IEEE Transactions on Intelligent Transportation Systems*, 11(2):348–358, 2010.

[4] J. Bhatti and T. E. Humphreys. Covert control of surface vessels via counterfeit civil gps signals. 2014.

[5] A. Broggi, M. Buzzoni, S. Debattisti, and P. Grisleri. Extensive Tests of Autonomous Driving Technologies. *IEEE Transactions on Intelligent Transportation Systems*, 14(3):1403–1415, 2013.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *20th USENIX conference on Security (SEC)*, pages 1–16, 2011.

[7] A. Faro, D. Giordano, and C. Spampinato. Adaptive Background Modeling Integrated With Luminosity Sensors and Occlusion Processing for Reliable Vehicle Detection. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1398–1412, 2011.

[8] L. Gomes. Hidden Obstacles for Google's Self-Driving Cars. `http://www.technologyreview.com/news/530276/hidden-obstacles-for-googles-self-driving-cars/`. Accessed: 2015-05-12.

[9] E. Guizzo. How google's self-driving car works. *IEEE Spectrum Online, October*, 18, 2011.

[10] K. Hall-Geisler. How Automatic Braking Systems Work. `http://auto.howstuffworks.com/under-the-hood/trends-innovations/automatic-braking-system.htm`. Accessed: 2015-05-12.

[11] A. Harvey. CV Dazzle: Camouflage from Computer Vision. http://ahprojects.com/projects/cv-dazzle. Accessed: 2015-05-12.

[12] T. Hoppe, S. Kiltz, and J. Dittmann. Security Threats to Automotive CAN Networks–Practical Examples and Selected Short-term Countermeasures. In *Computer Safety, Reliability, and Security*, pages 235–248. 2008.

[13] Ibeo. ibeo Lux 2010 - Technical Facts. http://www.autonomoustuff.com/uploads/9/6/0/5/9605198/ibeo_lux_as.pdf. Accessed: 2015-05-12.

[14] Y. Kang, K. Yamaguchi, T. Naito, and Y. Ninomiya. Multiband Image Segmentation and Object Recognition for Understanding Road Scenes. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1423–1433, Dec. 2011.

[15] C. Keller and M. Enzweiler. The benefits of dense stereo for pedestrian detection. *IEEE Transactions on Intelligent Transportation Systems*, 12(4):1096–1106, 2011.

[16] P. Kleberger, N. Nowdehi, and T. Olovsson. Towards designing secure in-vehicle network architectures using community detection algorithms. In *IEEE Vehicular Networking Conference (VNC)*, pages 69–76, 2014.

[17] H. Kong, S. Sarma, and F. Tang. Generalizing Laplacian of Gaussian filters for vanishing-point detection. *IEEE Transactions on Intelligent Transportation Systems*, 14(1):408–418, 2013.

[18] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental Security Analysis of a Modern Automobile. In *IEEE Symposium on Security and Privacy*, pages 447–462, 2010.

[19] J. Levinson, J. Askeland, J. Becker, J. Dolson, D. Held, S. Kammel, J. Z. Kolter, D. Langer, O. Pink, V. Pratt, et al. Towards fully autonomous driving: Systems and algorithms. In *IEEE Intelligent Vehicles Symposium (IV)*, pages 163–168, 2011.

[20] J. Lim, O. Tsimhoni, and Y. Liu. Investigation of Driver Performance With Night Vision and Pedestrian Detection Systems – Part I: Empirical Study on Visual Clutter and Glance Behavior. *IEEE Transactions on Intelligent Transportation Systems*, 11(3):670–677, 2010.

[21] X. Mao and D. Inoue. Demonstration of In-Car Doppler Laser Radar at 1.55 μm for Range and Speed Measurement. *IEEE Transactions on Intelligent Transportation Systems*, 14(2):599–607, 2013.

[22] C. Miller and C. Valasek. A survey of remote automotive attack surfaces. In *Black Hat USA*, 2014.

[23] MobilEye. About MobilEye. http://www.mobileye.com/about/. Accessed: 2015-05-12.

[24] A. Mogelmose. Vision-based traffic sign detection and analysis for intelligent driver assistance systems: Perspectives and survey. *IEEE Transactions on Intelligent Transportation Systems*, 13(4):1484–1497, 2012.

[25] F. Mujica. Scalable electronics driving autonomous vehicle technologies. Technical report, Autonomous Vehicles R&D, Kilby Labs, Texas Instruments, 2014. [Online]. [Accessed: April 2015] http://www.ti.com/lit/wp/sszy010a/sszy010a.pdf.

[26] A. Nguyen, J. Yosinski, and J. Clune. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images. In *IEEE Computer Vision and Pattern Recognition (CVPR)*, 2015.

[27] M. Obst, L. Hobert, and P. Reisdorf. Multi-sensor data fusion for checking plausibility of v2v communications by vision-based multiple-object tracking. In *IEEE Vehicular Networking Conference (VNC)*, pages 143–150, 2014.

[28] J. Petit, M. Feiri, and F. Kargl. Revisiting attacker model for smart vehicles. In *IEEE 6th International Symposium on Wireless Vehicular Communications (WiVeC)*, pages 1–5, 2014.

[29] J. Petit and S. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, 2015.

[30] S. Pu, M. Rutzinger, G. Vosselman, and S. O. Elberink. Recognizing basic structures from mobile laser scanning data for road inventory studies. *ISPRS Journal of Photogrammetry and Remote Sensing*, 66(6, Supplement):S28–S39, 2011. Advances in LIDAR Data Processing and Applications.

[31] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar. Security and Privacy Vulnerabilities of In-car Wireless Networks: a Tire Pressure Monitoring System Case Study. In *19th USENIX conference on Security (USENIX Security)*, pages 1–16, 2010.

[32] SAE International. Surface Vehicle Information Report J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. January 17, 2014.

[33] A. Samman, L. Rimai, J. R. McBride, R. O. Carter, W. H. Weber, and C. Gmachl. Potential use of near, mid and far infrared laser diodes in automotive LIDAR applications. *Vehicular Technology Conference*, 5:2084–2089, 2000.

[34] C. Stiller and J. Ziegler. 3d perception and planning for self-driving and cooperative automobiles. In *9th IEEE International Multi-Conference onSystems, Signals and Devices (SSD)*, pages 1–7, 2012.

[35] I. Tang and T. P. Breckon. Automatic Road Environment Classification. *IEEE Transactions on Intelligent Transportation Systems*, 12(2):476–484, June 2011.

[36] M. Wolf, A. Weimerskirch, and C. Paar. Security in Automotive Bus Systems. In *Workshop on Embedded IT-Security in Cars*, pages 11–12, 2004.

[37] W. Zhang and Q. Wu. Tracking and pairing vehicle headlight in night scenes. *IEEE Transactions on Intelligent Transportation Systems*, 13(1):140–153, 2012.

[38] M. Ziari, W. H. Steier, P. M. Ranon, S. Trivedi, and M. B. Klein. Photorefractivity in vanadium-doped ZnTe. *Applied physics letters*, 60(9):1052–1054, 1992.