SELF-DRIVING AND CONNECTED CARS: FOOLING SENSORS AND TRACKING DRIVERS

Jonathan Petit
AUTOMATED/CONNECTED VEHICLE

GPS, 802.11p

LIDAR

Camera

RADAR

wheel encoder

On-Board Unit, emaps

ultrasonic sensors
Levels of Driving Automation (SAE J3016)

- **No Automation**: Human driver monitors the driving environment.
- **Driver Assistance**: Automated driving system monitors the driving environment.
- **Partial Automation**: Conditional automation.
- **Conditional Automation**: High automation.
- **High Automation**: Full automation.

With the goal of providing common terminology for automated driving, SAE International's new standard J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, delivers a harmonized classification system and supporting definitions that:

- Identify six levels of driving automation from "no automation" to "full automation".
- Base definitions and levels on functional aspects of technology.
- Describe categorical distinctions for a step-wise progression through the levels.
- Are consistent with current industry practice.
- Eliminate confusion and are useful across numerous disciplines (engineering, legal, media, and public discourse).
- Educate a wider community by clarifying for each level what role (if any) drivers have in performing the dynamic driving task while a driving automation system is engaged.

Learn more about SAE J3016 or purchase the standard document: www.sae.org/autodrive
REMOTE ATTACKS ON AUTOMATED VEHICLES SENSORS:
EXPERIMENTS ON CAMERA AND LIDAR

Jonathan Petit, Bas Stottelaar, Michael Feiri, Frank Kargl
ATTACKING AUTONOMOUS VEHICLE SENSORS

GPS, 802.11p

LIDAR

Camera

RADAR

wheel encoder

On-Board Unit, emaps

ultrasonic sensors

On-Board Unit, eMaps
CAMERA

- MobilEye C2-270
- Features:
  - Lane departure
  - Rear collision alert
  - Pedestrian alert

Aptina MT9V024 CMOS
Red/Clear camera
752x480 at 60 FPS
ATTACKING CAMERA

- Attacks:
  - Jamming
  - **Blinding**
  - Scenery attack

- Equipments:
  - Light sources (LED, laser)
  - Screen
ATTACKING CAMERA - SENSITIVITY

- Ledsee 650 nm diode point laser with focusable lens.
- Max. output: 5 mW.
- Distance: 1 m
ATTACKING CAMERA - SENSITIVITY

- Ledsee 650 nm diode point laser with focusable lens.
- Max. output: 5 mW.
- Distance: 1 m

Tonal distribution
ATTACKING CAMERA - SENSITIVITY

• LED 850nm
• LED 860nm
• LED 875nm
• LED 880nm
• Laser 905nm
• LED 940nm
• Matrix LED 940nm
BLINDING CAMERA

- Use auto exposure
- “Time to recover”
BLINDING CAMERA

Video of different light sources and their impact on camera
BLINDING CAMERA

- White spot, light, 50cm
- Affect background

Tonal distribution
BLINDING CAMERA

- White spot, light, 50cm
- Affect background
BLINDING CAMERA

Video of MobilEye C2-270 blinded by laser 650 nm

• Laser 650nm
BLINDING CAMERA

Video of MobilEye C2-270 blinded by laser 650 nm

- Laser 650nm
DAZZLER
Laser Weapon 300mW Green laser Dazzler

$850.00

Add to Cart: 1

100% IR FILTERED!
Intelligent Focusable Mechanism
Weapon mountable for versatility
Non-lethal crowd control and tactical area denial
CE/FDA/ROHS CERTIFIED

One Year's Guarantee!
COUNTERMEASURES
CAMERA

• Increase redundancy by adding cameras to overlap fully or partially.

• Limit the effects of high-intensity light sources on image sensors via certain optics and materials.

• Detect jamming attacks on cameras via spectral analysis.
LIDAR

• **IBEO LUX 3**
  • 200 meters range
  • Viewing angle 110°
  • 4 layers
  • Up to 3 echoes
  • Scanning speeds: 12.5/25/50 Hz
  • Angular resolution: up to 0.125° horizontal
  • Distance resolution: 4 cm
  • Detect object
  • Object tracking
Ibeo LUX 3
Battery
Control Box
HOW DOES LIDAR WORK?
HOW DOES LIDAR WORK?

50Hz pulse
HOW DOES LIDAR WORK?

1.41 cm  0.73 cm

1.41 cm  0.96 cm
ATTACKING LIDAR

• Attacks:
  • Replay
  • Relay
  • Jamming
  • Spoofing
  • Tracking

• Equipments:
  • Receiver/Transmitter
  • Pulse generators
Emitting laser: Osram SPL-PL90 ($43.25)
Max. output: 25W for 100 ns
Viewing angle: 9°

Receiving photodetector: Osram SFH-213 ($0.65)
SETUP

HP 8011A

Philips PM5715
Video demonstrating “flashlight”
SPOOFING LIDAR (1/3)

0 s

Attack window
(one scan step)

1.33 µs

Injected Reflection
(Second Echo)

Silent window
(gap)

X ms

Undetected Injected Reflection

Actual Reflection
(First Echo)

Time
SPOOFING LIDAR (2/3)

Original signal

Delay output

Counterfeit signal

Delay

Number of copies

Number of pulses

Time
SPOOFING LIDAR (3/3)

Video demonstrating advanced spoofing on LiDAR
TRACKING LIDAR

Video demonstrating impact of spoofing on tracking box
COUNTERMEASURES LIDAR

• Use multiple lasers with non-overlapping wavelengths for redundancy:
  **Ibeo:** Possible, but currently not preferred by Ibeo

• Shorten the pulse period by limiting the maximum range:
  **Ibeo:** Today Ibeo adapts the maximum range according to the environmental situation
Countermeasures LIDAR

• Introduce random probing - In preparation by Ibeo:
  – Prevents spoofing - spoofing only generates uncorrelated noise but no validated tracks
  – Enables the detection of spoofing attacks

• Probe multiple times to raise the confidence in a measurement:
  – Already implemented by object tracking with dedicated track validation on sensor object output for vehicle control systems

• Increase the number of objects than can be tracked (65 here):
  – Just a question of processing power, today Ibeos systems are able to manage up to 1,023 objects simultaneously
Countermeasures LIDAR - System Setup Analyzed

Meas core (Standard probing)

Raw data preprocessing

Object tracking

Object Track Validation

Developer Interface

Vehicle Control
Countermeasures LIDAR - System Setup in Preparation

Meas core (Random probing)

Raw data preprocessing

Object tracking

Object Track Validation

Vehicle Control

Spoofing Detection
BLACK HAT SOUND BYTES.

1. Fooling LiDAR on raw data level in laboratory environment is possible but establishing stable objects on sensor output in real driving scenarios level for vehicle control could not be demonstrated.

2. Fooling camera-based systems is easy and cheap.

3. Don’t trust automated vehicle sensors unless you implement countermeasures to mitigate such threats.
CONNECTED VEHICLES: SURVEILLANCE THREAT AND MITIGATIONS

Jonathan Petit, Djurre Broekhuis, Michael Feiri, Frank Kargl
They Are Watching You, 2004, Linda Braucht (20th C American) Computer graphics
They Are Watching You

Linda Braucht (20th C. American) Computer graphics
They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics
They Are Watching You 2004 Linda Braucht (20th C. American) Computer graphics
AUTOMATED/CONNECTED VEHICLE

- GPS, 802.11p
- LIDAR
- Camera
- RADAR
- Wheel encoder
- On-Board Unit, emaps
- Ultrasonic sensors
APPLICATION AREAS FOR V2X COMMUNICATION

Safety

Efficiency

Comfort
CONTENT OF BEACON

<table>
<thead>
<tr>
<th>0</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Station ID</td>
<td>Sequence Number</td>
</tr>
<tr>
<td>Timestamp</td>
<td></td>
</tr>
<tr>
<td>Latitude</td>
<td></td>
</tr>
<tr>
<td>Longitude</td>
<td></td>
</tr>
<tr>
<td>Speed</td>
<td>Bearing</td>
</tr>
<tr>
<td>Latitude error</td>
<td>Longitude error</td>
</tr>
<tr>
<td>Velocity Error</td>
<td>Bearing Error</td>
</tr>
</tbody>
</table>

36
Beacons are broadcast within 300 m in clear!

<table>
<thead>
<tr>
<th>Station ID</th>
<th>Sequence Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>Bearing</td>
</tr>
<tr>
<td>Latitude error</td>
<td>Longitude error</td>
</tr>
<tr>
<td>Velocity Error</td>
<td>Bearing Error</td>
</tr>
</tbody>
</table>
**CONTENT OF BEACON**

Beacons are broadcast within 300 m in clear!

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Station ID</td>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Speed</td>
<td>Bearing</td>
<td></td>
</tr>
<tr>
<td>Latitude error</td>
<td>Longitude</td>
<td></td>
</tr>
<tr>
<td>Velocity Error</td>
<td>Bearing Error</td>
<td></td>
</tr>
</tbody>
</table>

- pathHistory
- last location parked
- seat belt use
- steering angle
- fuel consumption
- exterior temperature
- ...

...
**CONTENT OF BEACON**

- pathHistory
- last location parked
- seat belt use
- steering angle
- fuel consumption
- exterior temperature

Beacons are broadcast within 300 m in clear!

“Automakers collect and wirelessly transmit driving history data to data centers” (Markey Report)
PRIVACY VIOLATIONS

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

collect information about me, my car, and my surroundings

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

In-vehicle Sensor Data

Processing

Data at rest

Malware

store information

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

sensor data

processing

data at rest

in-vehicle

malware

store information

location tracking, break forward secrecy

PRIVACY VIOLATIONS

collect information about me, my car, and my surroundings

store information

privacy inferences

I can track you!

I'm here!

I'm here!

I'm here!
Attacker Model
- Mid-sized / Hobbyist
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking
Attacker Model
- Mid-sized / Hobbyist
- Passive
- External
- Trip-level tracking period
- Road/Zone-level tracking

Let’s track the security guard vehicle!
EXPERIMENTAL SETUP (1/4)
EXPERIMENTAL SETUP (1/4)

- Nexcom VTC6201
- Intel Atom D510 processor
- Unex CM10-HI Mini-PCI 802.11 a/b/g module with custom drivers for 802.11p
- 2 x MobileMark ECOM9-5500 (high gain 9dBi) 5.0-6.0 GHz antennas
- one SMA connector for GPS
- Ubuntu 12.04
EXPERIMENTAL SETUP (2/4)
EXPERIMENTAL SETUP (3/4)
Where should an attacker deploy sniffing stations?

Intersections
Busiest intersections
Highest degree
Articulation points
**Intersection A**
Ground floor
75 m from intersection
2 x Smarteq V09/54 antennas (9 dBi gain)

**Intersection B**
1st floor
110 m from intersection
2 x Smarteq V09/54 antennas (9 dBi gain)
ZONE-LEVEL TRACKING
The equipment was deployed for 16 days during which the vehicle transmitted 2,734,691 messages and we eavesdropped on 68,542 messages.
Corresponds to 3.17% of all messages sent
Corresponds to 3.17% of all messages sent

Zone-level tracking: 72.82%
TRACKING ACCURACY (MLZ)
## Tracking Accuracy (MLZ)

<table>
<thead>
<tr>
<th># of intersections</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>61.12%</td>
<td>72.82%</td>
<td>81.40%</td>
<td>84.26%</td>
<td>95.28%</td>
</tr>
<tr>
<td>2</td>
<td>67.49%</td>
<td>73.42%</td>
<td>78.96%</td>
<td>89.51%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>58.10%</td>
<td>67.41%</td>
<td>81.53%</td>
<td>86.41%</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>52.53%</td>
<td>69.98%</td>
<td>73.15%</td>
<td>86.58%</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>54.85%</td>
<td>73.32%</td>
<td>77.44%</td>
<td>87.29%</td>
<td></td>
</tr>
</tbody>
</table>

### Average

|        | 58.82% | 69.55% | 78.25% | 86.81% | 95.28% |
TRACKING ACCURACY (MLR)
TRACKING ACCURACY (MLR)

- Maximum coverage
- Mean coverage

Samples covered (%)

Number of observed intersections
Can we stop tracking?
CANDIDATE SOLUTIONS

- Cloaking/Fuzzing location
- Anonymous credentials
- Encryption
- Opt-out
- Pseudonyms
IEEE and ETSI mention the need to
“use a pseudonym that cannot be linked to [...] the user’s true identity” and suggest to change it frequently “[...] to avoid simple correlation between the pseudonym and the vehicle”
Pseudonym Lifecycle

1. Enroll vehicle
2. Issue VID cert.
3. Authenticate with VID
4. Retain VID-pseudonym mapping
5. Issue pseudonym certificates
6. Sign messages w/ pseudonym cert.
7. Change active pseudonym / request new pseudonyms
8. Obtain pseudonym cert. to resolve
9. Request pseudonym resolution
10. Return identity information
11. Revoke VID

- Pseudonym issuance
- Pseudonym resolution
- Pseudonym use
- Pseudonym change
- Pseudonym revocation

Pseudonym use: Pseudonyms are used to sign every outgoing packet. Public/private keys of previously obtained pseudonyms are stored and managed by a Hardware Security Module (HSM), which is tamper-resistant to restrict the parallel usage of pseudonyms [Papadimitratos et al. 2008]. The pseudonym restriction scheme (lifetime, amount of pseudonyms in parallel, etc.) is dependent on the assurance level of the HSM [Schweppe et al. 2011]. For example, the available secure storage space impacts the number of pseudonyms that could be stored in parallel inside the HSM. For signing or encryption tasks only the currently valid pseudonym certificates can be used or those that are exposed for use by the HSM.

- Pseudonym change: A pseudonym has a lifetime to hamper tracking based on longterm pseudonyms. When a pseudonym expires, the OBU loads a new pseudonym from its store or requests new pseudonyms from the pseudonym provider, which corresponds to pseudonym issuance. In the first case, pseudonyms are changed according to the current context by the vehicle while driving. The employed pseudonym change strategy is crucial to prevent linking of pseudonyms when changing. Numerous pseudonym change strategies have been proposed, which we detail separately in Section 3.3.

- Pseudonym resolution: Pseudonym-identity resolution is performed by pseudonym resolution. Law enforcement / resolution auth.

Assume perfect pseudonym change
Potential re-identification from other channels
PRIVACY LOSS FUNCTION

\[ P_{\text{pnm}}(t) = \begin{cases} 
\max(P_{\text{pnm}}(t-1) - \sum_{i=1}^{N_{\text{veh}}} p_i \cdot \log p_i, P_{\text{pmax}}) & \text{if } t \in T_{\text{upc}} \\
0 & \text{if } t \in T_{\text{obs}} \end{cases} \]

Pseudonym changes

\[ P_{\text{int}}(t) = \begin{cases} 
\max(P_{\text{int}}(t-1) - \sum_{j=1}^{N_{\text{road}}} p_j \cdot \log p_j, P_{\text{rmax}}) & \text{if } t \in T_{\text{ui}} \\
0 & \text{if } t \in T_{\text{obs}} \end{cases} \]

Unobserved intersections

\[ P_{\text{road}}(t) = \begin{cases} 
\max(P_{\text{road}}(t-1) + \lambda(t_{\text{last}} - t), P_{\text{dmax}}) & \text{if } t \in T_{\text{urs}} \\
0 & \text{if } t \in T_{\text{obs}} \end{cases} \]

Time since observation

\[ P(t) = P_{\text{pnm}}(t) + P_{\text{int}}(t) + P_{\text{road}}(t) \]

Total
EVOLUTION OF PRIVACY LEVEL
2 sniffing stations
Pseudonym change every 5 min
8 sniffing stations
Pseudonym change every 5 min
8 sniffing stations
Pseudonym change every 5 min

**Road-level tracking:** 90%
PSEUDONYM CHANGE STRATEGIES

Normalized privacy level with pseudonyms

- 5s
- 100s
- 300s
- 1000s
- 2500s
- trip
- none

Number of observed intersections

Normalized privacy level

59
PSEUDONYM CHANGE STRATEGIES

Normalized privacy level with pseudonyms

Number of observed intersections

Normalized privacy level

- 5s
- 100s
- 300s
- 1000s
- 2500s
- trip
- none
# COST MODEL

<table>
<thead>
<tr>
<th>#observed intersection</th>
<th>Equipment Cost (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>500</td>
</tr>
<tr>
<td>2</td>
<td>1000</td>
</tr>
<tr>
<td>8</td>
<td>4000</td>
</tr>
<tr>
<td>Full campus</td>
<td>10500</td>
</tr>
</tbody>
</table>

6000€/km²
+ installation/operational/maintenance cost

Expect price drop!
(Raspberry Pi or SDR: http://wime-project.net/)
CONCLUSION OF THE EXPERIMENT

Additional mitigations: silent period, encrypted BSMs, ...

Generalization
large-scale scenarios

Privacy-Preserving Road Networks?
BLACK HAT SOUND BYTES.

1. **Everyone** can deploy a surveillance system to track connected vehicles. It is *cheap* and *easy* and somewhat effective.

2. Countermeasures exist to *mitigate* the risk.
Questions & Answers
Jonathan Petit
jpetit@securityinnovation.com

Check out our white papers!
contain URL to results/videos!