SURVEY OF AUTOMOTIVE PRIVACY REGULATIONS AND PRIVACY-RELATED ATTACKS

Mert D. Pesé, Kang G. Shin
Real-Time Computing Laboratory (RTCL)
University of Michigan – Ann Arbor

SAE INTERNATIONAL®

COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

Agenda

Introduction

Background

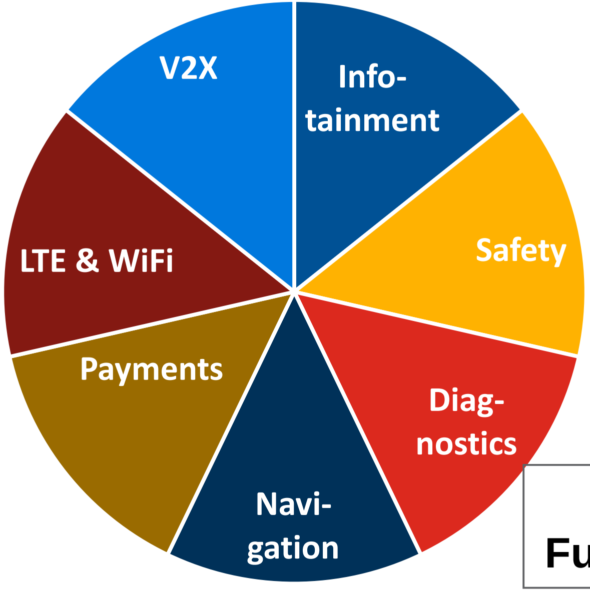
Privacy Regulations

Privacy Attacks

Risk Assessment

Conclusion

Introduction



2020s

CV Functionalities

Data Connectivity

- 78 million vehicles as of 2018
- 98% of all new vehicles in US and Europe by 2021

Privacy Concerns

- Facebook-Cambridge Analytica incident
- General Data Protection Regulation (GDPR)

Agenda

Introduction

Background

Privacy Regulations

Privacy Attacks

Risk Assessment

Conclusion

Who collects what data?

WHO?

BMW CarData

Mercedes me connect

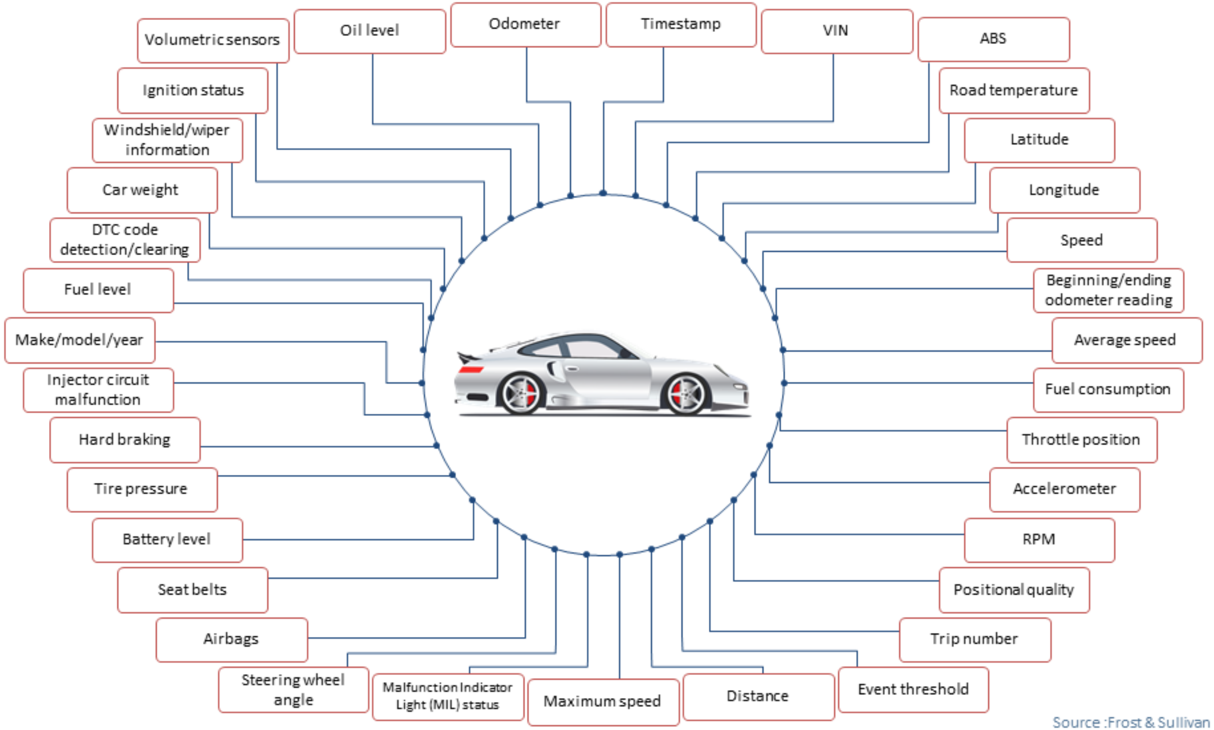
PROGRESSIVE

State Farm

verizon

otonomo

WHAT?



Source :Frost & Sullivan

How is data collected?

OBD-II Dongle

Source: Progressive

Source: Vyncs

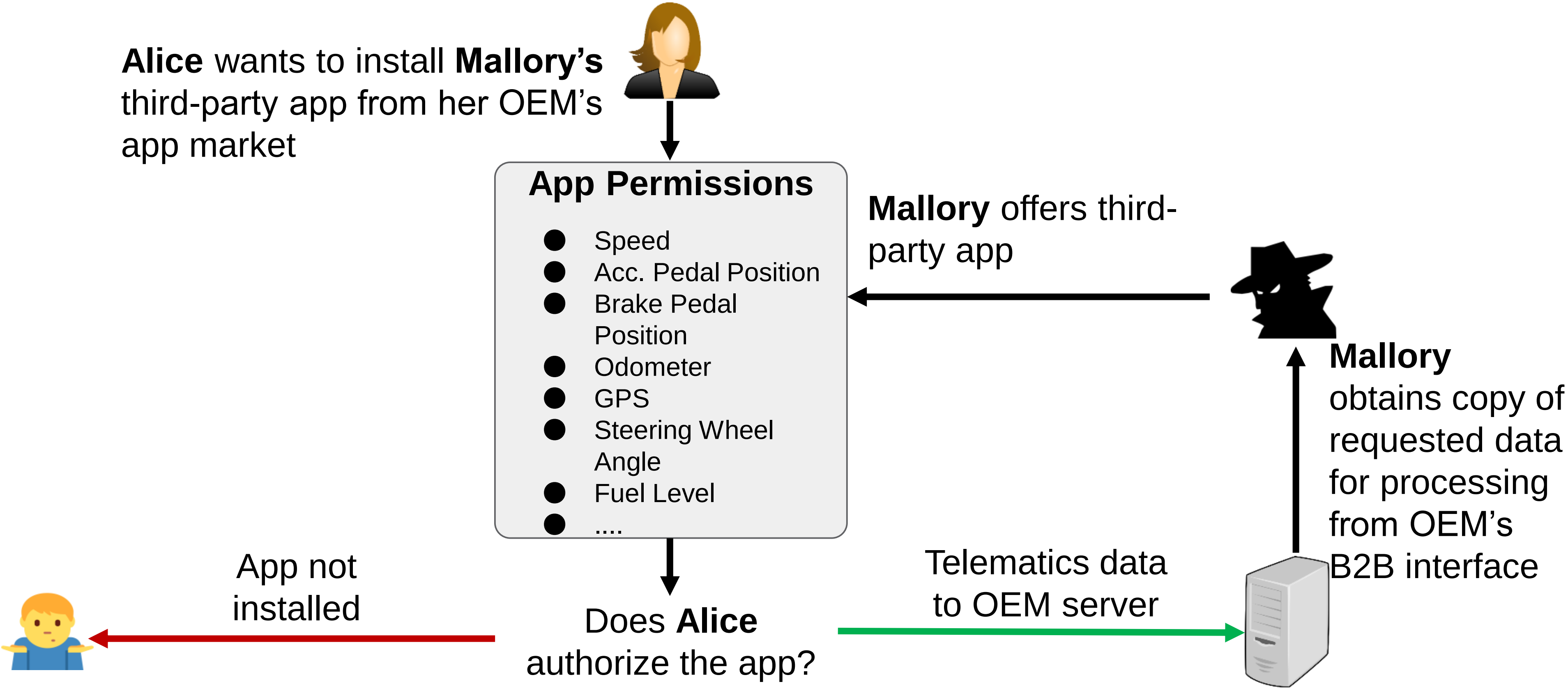
CarLab

Source: RTCL, University of Michigan

OEM Telematic Platform

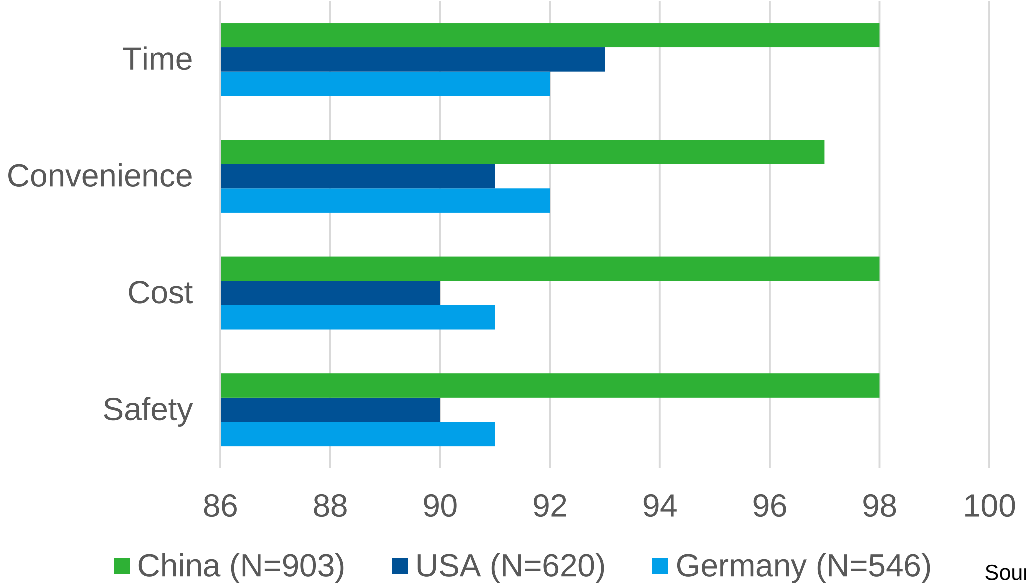
Source: Audi

Threat Model



Willingness of sharing vehicle data is high!

Willingness to share data: Which of the following use-cases would you prefer?

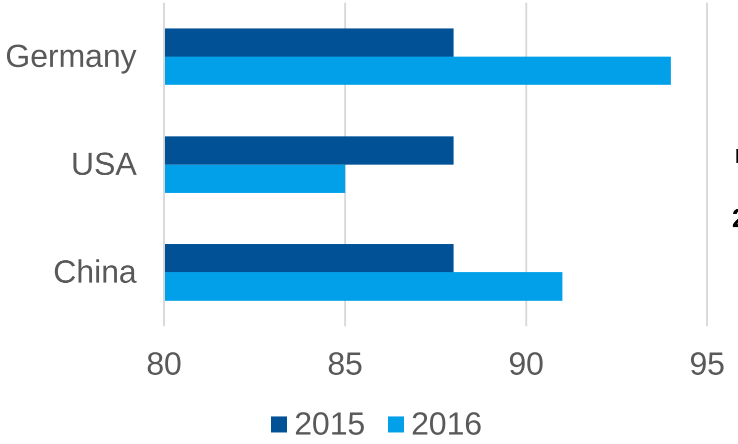


Source: McKinsey & Company

Across geographies, willingness to share data and pay for time-saving use-cases is high

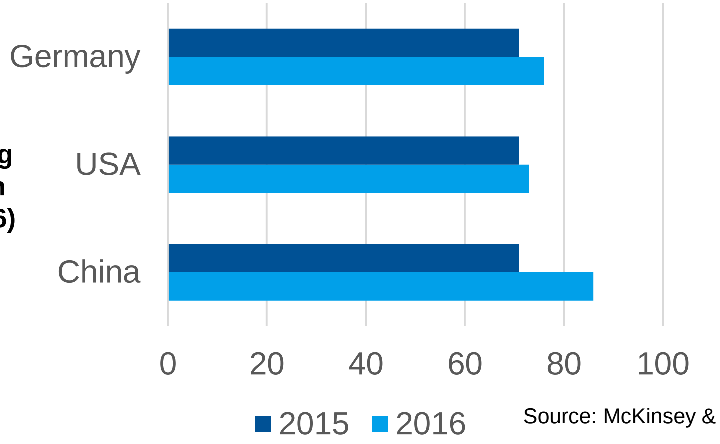
Privacy-awareness is also high!

Are you aware that certain data is openly accessible to applications and shared with 3rd parties?



Do you consciously decide to grant certain applications access to your personal data, even if you may have generally disabled this access for other applications?

Percentage of respondents saying "Yes", N = 3000 (in 2015), 3186 (in 2016)



Source: McKinsey & Company

Customers' awareness of how applications access and share personal data is high as is their willingness to trade data for benefits

Agenda

Introduction

Background

Privacy Regulations

Privacy Attacks

Risk Assessment

Conclusion

Privacy Regulations

Voluntary guidelines from 2014

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS, INC.

Consumer Privacy Protection Principles

PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES

November 12, 2014

OEMs only have to ask permission for three categories:

- Driving behavior
- Geolocation
- Biometrics

"covered information"

US Congress: Driver Privacy Act of 2015

- Deals only with EDR data

S.766 - Driver Privacy Act of 2015
114th Congress (2015-2016)

BILL Hide Overview ✖

Sponsor:	Sen. Hoeven, John [R-ND] (Introduced 03/17/2015)
Committees:	Senate - Commerce, Science, and Transportation
Committee Reports:	S. Rept. 114-147

Agenda

Introduction

Background

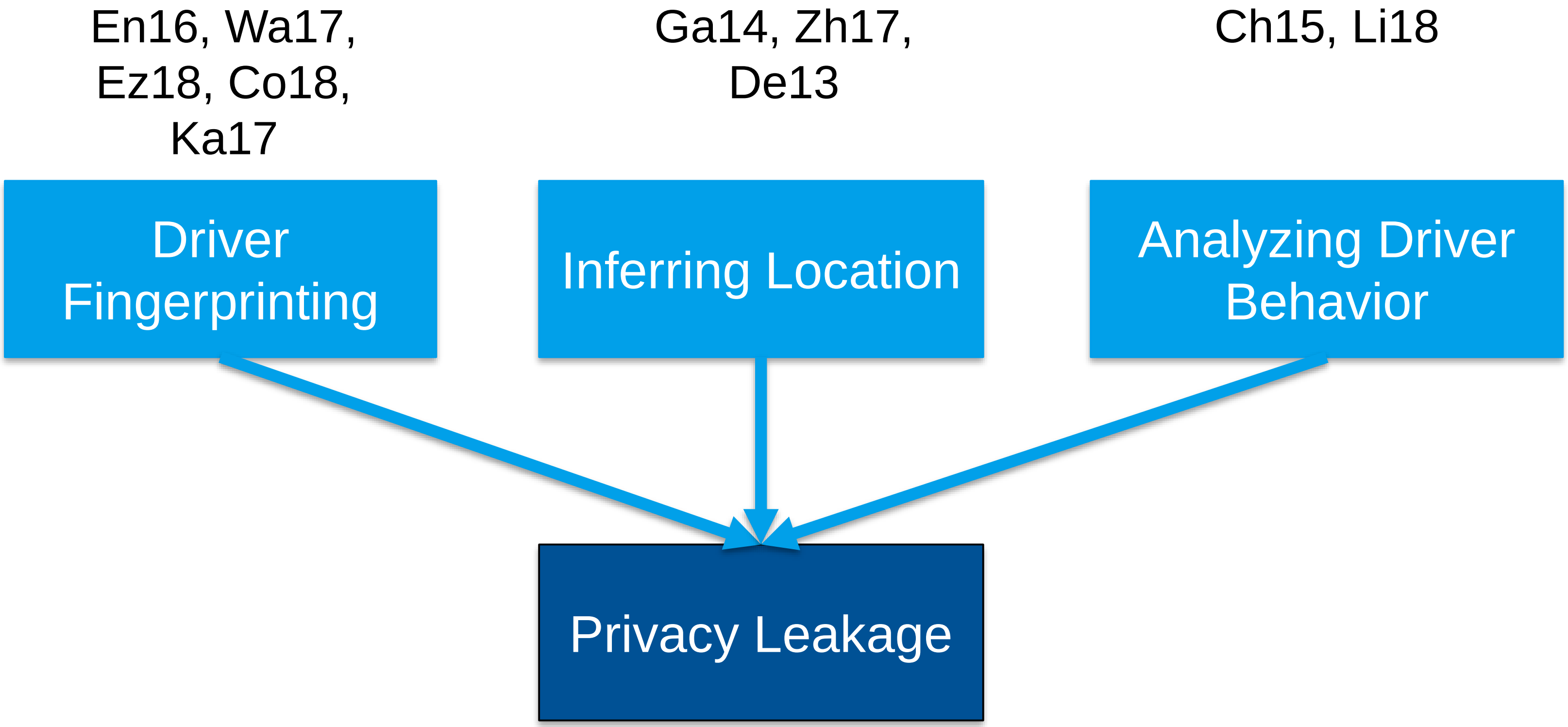
Privacy Regulations

Privacy Attacks

Risk Assessment

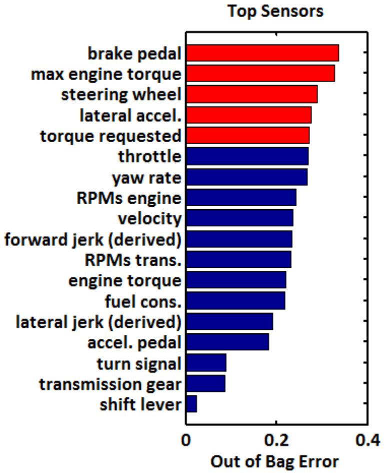
Conclusion

Privacy Attacks



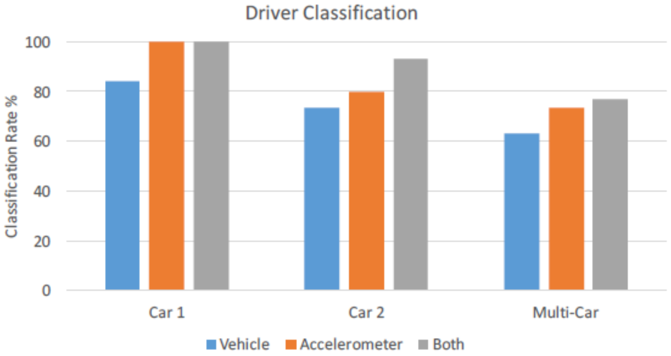
Driver fingerprinting (selection)

[En16]: Identify 15 drivers using 15 vehicular sensors with 100% accuracy



Enev, M. et al., “Automobile Driver Fingerprinting,” Proceedings on Privacy Enhancing Technologies 1:34-50, 2016.

[Co18]: Uses mobile and vehicular sensors; Less than 81% accuracy with latter



Corbett, Cherita, Alexis Jimmy, and Watkins Lanier, “Who’s Driving You?,” Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual, 1-4, IEEE, 2018.

Driver fingerprinting (selection)

[Ka17]: Identify 24 drivers with 90% accuracy in 20s only using pre-trip data

Pre-trip Fields	Frequency (Hz)	Range	Driving Fields	Frequency (Hz)	Range
Door status (DO & DC)	10	Boolean	Brake pedal (BP)	10	0-100
Ignition switch status (ISU)	10	Boolean	Accelerator pedal (AP)	50	0-100
Seatbelt status (SF)	10	Boolean	Revolutions per minute (RPM)	10	0-16000
Shifter position (SU)	40	Integer(1-6,13,14,15)	Throttle position (TP)	10	0-100
Parking brake active	100	Boolean	Turn signals (TS)	Event	Boolean
			Vehicle velocity (V)	10	0-255 kmh
			Steering wheel angle (SWA)	100	0-1340°

Kar, Gorkem, Jain Shubham, Gruteser Marco, Chen Jinzhu, Bai Fan, and Govindan Ramesh, “PredriveID: Pre-Trip Driver Identification from In-Vehicle Data,” in Proceedings of the Second ACM/IEEE Symposium on Edge Computing, 2, ACM, 2017.

Location Inference (selection)

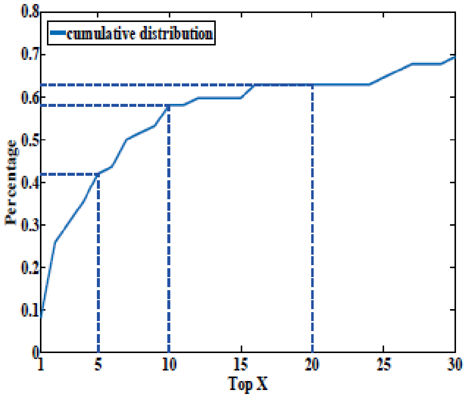
[De13]: Using speed from tracking unit with 37% accuracy

Dewri, R., Annadata, P., Eltarjaman, W., and Thurimella, R., "Inferring Trip Destinations from Driving Habits Data," in Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society, 267-272, ACM, November 2013).

trip length (miles)	number of candidates	rank of actual destination
1.48	12	1
1.59	12	1
2.60	50	1
3.23	15	1
3.78	11	2
3.85	23	1
3.93	52	1
3.93	49	1
3.95	37	3
5.47	11	2
5.89	18	1
5.84	20	1
7.95	196	2
9.42	26	4
13.15	37	3
14.10	53	1
14.57	68	1
24.10	42	13

[Zh17]: Using speed from OBD-II dongle with 70% accuracy of correct path being in Top 30 of generated candidate paths

Zhou, L., Chen, Q., Luo, Z., Zhu, H., and Chen, C. (June 2017). Speed-Based Location Tracking in Usage-Based Automotive Insurance, in Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on, 2252-2257, IEEE.



Driving Behavior Analysis

Usage-Based Insurance (UBI): Adjust insurance premium based on driving behavior

Company	Mileage	Speed	Acceleration	Hard Braking	Turns
Progressive	✔	✔		✔	
State Farm	✔	✔	✔	✔	✔
Allstate	✔	✔		✔	
Esurance		✔	✔	✔	

[Ch15, Li18]: Safe or distracted driving detection

Chen, S.H., Pan, J.S., and Kaixuan, L., "Driving behavior Analysis Based on Vehicle OBD Information and Adaboost Algorithms," in Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, 18-20, 2015.

Li, Z., Bao, S., Kolmanovsky, I.V., and Yin, X., "Visual-Manual Distraction Detection Using Driving Performance Indicators with Naturalistic Driving Data," IEEE Transactions on Intelligent Transportation Systems, 2017.

Agenda

Introduction

Background

Privacy Regulations

Privacy Attacks

Risk Assessment

Conclusion

How can we quantify the privacy risk of a vehicular sensor?

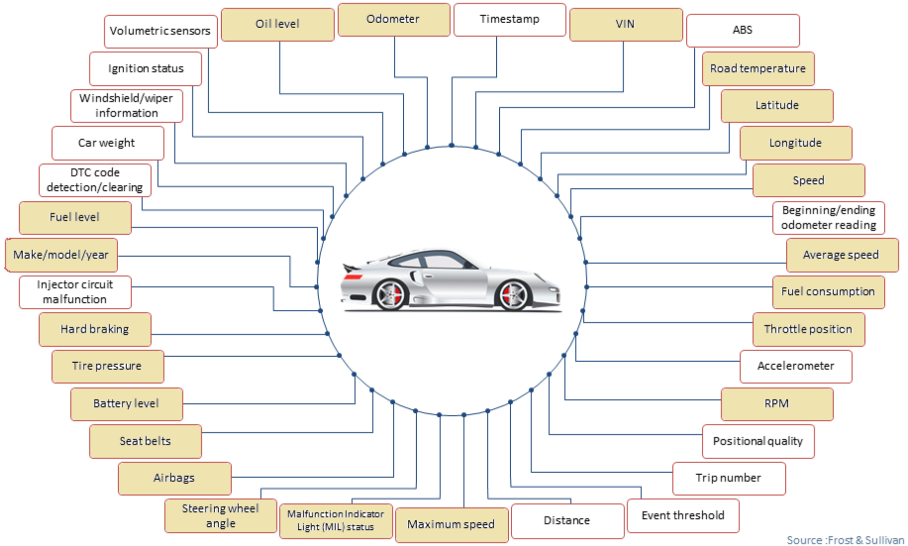
Define a 3-tuple

(Driver Fingerprinting, Location Inferencing, Driving Behavior Analysis)

For each of the 20 sensors, assign

- ❖ Boolean 1 if sensor contributes to attack category
- ❖ Boolean 0 if not

<u>Example:</u> Current Speed (0,1,0)



Source :Frost & Sullivan

Risk Assessment

How can we quantify the privacy risk of a vehicular sensor?

Some attacks are only possible through a combination of multiple sensors

Inspect sensors pairwise in their contribution to attack categories

↓

Symmetric 20x20 Risk Matrix

↓

Privacy Score

Risk Matrix – Part 1

	Odometer	VIN	Outside Temperature	GPS	Current Speed	Average Speed	Maximum Speed	Fuel Consumption	Throttle Position	RPM	Steering wheel angle	Airbag status	Seat belt status	Battery level	Tire pressure	Hard braking	Make/Model/Year	Fuel level	Check engine light on	Oil level
Odometer	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/1	0/0/0	0/0/1	0/0/1	0/0/0	0/0/1	0/0/0	0/0/0
VIN	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Outside Temperature	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Location (GPS)	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1	1/1/1
Current Speed	0/1/0	0/1/1	0/1/0	1/1/1	0/1/0	0/1/0	0/1/0	1/1/0	0/1/1	0/1/1	0/1/1	0/1/0	0/1/1	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0
Average Speed	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Maximum Speed	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Fuel Consumption	0/0/1	0/0/1	0/0/0	1/1/1	1/1/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0
Throttle Position	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/1	0/0/0	0/0/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
RPM	0/0/0	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0

Risk Matrix – Part 2

	Odometer	VIN	Outside Temperature	GPS	Current Speed	Average Speed	Maximum Speed	Fuel Consumption	Throttle Position	RPM	Steering wheel angle	Airbag status	Seat belt status	Battery level	Tire pressure	Hard braking	Make/Model/Year	Fuel level	Check engine light on	Oil level
Steering wheel angle	0/1/0	0/1/0	0/1/0	1/1/1	0/1/1	0/1/0	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0	0/1/0	0/1/0	0/1/1	0/1/0	0/1/0	0/1/0	0/1/0
Airbag status	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
Seat belt status	0/0/1	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/1/0	0/0/1	0/0/1	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0
Battery level	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Tire pressure	0/0/1	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Hard braking	0/0/1	0/0/0	0/0/0	1/1/1	0/1/1	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/1/1	0/0/1	0/0/1	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Make/Model/Year	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Fuel level	0/0/1	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/1	0/0/0	0/0/0
Check engine light on	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0
Oil level	0/0/0	0/0/0	0/0/0	1/1/1	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/1/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0	0/0/0

Risk Matrix (selection)

GPS is a very sensitive sensor, it contributes to all attack categories in combination with any sensor

	Odometer	VIN	Outside Temperature	GPS	Current Speed
Odometer	0/0/0	0/0/0	0/0/0	**1/1/1**	0/1/0
VIN	0/0/0	0/0/0	0/0/0	**1/1/1**	0/**1/1**
Outside Temperature	0/0/0	0/0/0	0/0/0	**1/1/1**	0/1/0
Location (GPS)	**1/1/1**	**1/1/1**	**1/1/1**	**1/1/1**	**1/1/1**
Current Speed	0/1/0	0/1/1	0/1/0	**1/1/1**	0/1/0

Current Speed contributes to location inference in any combination

Risk Assessment

How can we quantify the privacy risk of a vehicular sensor?

↓

Symmetric 20x20 Risk Matrix

↓

Privacy Score

Privacy Score

Metric defining privacy risk of sensor *k*:

$$PS_k = \frac{\sum_i \sum_j w_i \, c^i_{k,j}}{N \sum_i w_i}$$

- **Evaluated for *N=20* sensors**
- ***i* is attack category**
- ***c* is 3-tuple entry in the matrix**
- **Weights w are optional (for evaluation assigned to 1)**

Normalized Privacy Score (NPS) to arrange values in interval [0,1]:

$$NPS_k = \frac{PS_k - \min(PS)}{\max(PS) - \min(PS)}$$

Privacy Score

Vehicular Sensor	Privacy Score (PS)	Normalized Privacy Score (NPS)
Location	1.00	1.00
Current Speed	0.48	0.43
Steering wheel angle	0.42	0.37
Fuel Consumption	0.18	0.11
Hard braking	0.18	0.11
Odometer	0.17	0.10
Seat belt status	0.17	0.10
Throttle Position	0.15	0.08
RPM	0.15	0.08
VIN	0.12	0.04
Airbag status	0.12	0.04
Fuel level	0.12	0.04
Tire pressure	0.10	0.02
Make/model/year	0.10	0.02
Outside Temperature	0.08	0.00
Average Speed	0.08	0.00
Maximum Speed	0.08	0.00
Battery level	0.08	0.00
Check engine light on	0.08	0.00
Oil level	0.08	0.00

Agenda

Introduction

Background

Privacy Regulations

Privacy Attacks

Risk Assessment

Conclusion

Conclusion

- ❖ Pervasiveness of vehicular data collection
- ❖ Lax privacy regulation in automotive domain

} Increased privacy risk

- ❖ Surveyed and categorized existing attacks
- ❖ Defined risk matrix to assess the risk of 20 sensors contributing to attack categories
- ❖ Quantified each sensor’s risk using Privacy Score (PS)
- ❖ Privacy Score can be used as design parameter of future automotive privacy-protection schemes

THANK YOU

Mert D. Pesé
University of Michigan – Ann Arbor
2260 Hayward Street, Ann Arbor, MI 48109-2121, U.S.A

(734) - 489 – 2825
mpese@umich.edu

References

[En16] Enev, M. et al., “Automobile Driver Fingerprinting,” Proceedings on Privacy Enhancing Technologies 1:34-50, 2016.

[Wa17] Bo, W., Panigrahi, S., Narsude, M., and Mohanty, A., “Driver Identification Using Vehicle Telematics Data,” SAE Technical Paper 2017-01-1372, 2017, doi:10.4271/2017-01-1372.

[Ez18] Ezzini, S., Berrada, I., and Ghogho, M., “Who is Behind the Wheel? Driver Identification and Fingerprinting,” Journal of Big Data 5(1):9, 2018.

[Co18] Corbett, Cherita, Alexis Jimmy, and Watkins Lanier, “Who’s Driving You?,” Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual, 1-4, IEEE, 2018.

[Ka17] Kar, Gorkem, Jain Shubham, Gruteser Marco, Chen Jinzhu, Bai Fan, and Govindan Ramesh, “PredriveID: Pre-Trip Driver Identification from In-Vehicle Data,” in Proceedings of the Second ACM/IEEE Symposium on Edge Computing, 2, ACM, 2017.

References

[Ga14] Gao, X., Firner, B., Sugrim, S., Kaiser-Pendergrast, V., Yang, Y., and Lindqvist, J., “Elastic Pathing: Your Speed is Enough to Track You,” in Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 975-986, ACM, September 2014.

[Zh17] Zhou, L., Chen, Q., Luo, Z., Zhu, H., and Chen, C. (June 2017). Speed-Based Location Tracking in Usage-Based Automotive Insurance, in Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on, 2252-2257, IEEE.

[De13] Dewri, R., Annadata, P., Eltarjaman, W., and Thurimella, R., “Inferring Trip Destinations from Driving Habits Data,” in Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society, 267-272, ACM, November 2013).

[Ch15] Chen, S.H., Pan, J.S., and Kaixuan, L., “Driving behavior Analysis Based on Vehicle OBD Information and Adaboost Algorithms,” in Proceedings of the International MultiConference of Engineers and Computer Scientists, vol. 1, 18-20, 2015.

References

[Li18] Li, Z., Bao, S., Kolmanovsky, I.V., and Yin, X., "Visual-Manual Distraction Detection Using Driving Performance Indicators with Naturalistic Driving Data," IEEE Transactions on Intelligent Transportation Systems, 2017.