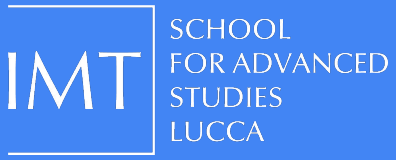
The SPADA Methodology for Privacy Threat Modelling

Giampaolo Bella and Mario Raciti

AUIN Workshop



15/11/23 – Online

Agenda

1. **Introduction**
2. **SPADA for Privacy Threat Modelling**
3. **Demonstration on Smart Cars**
4. **Conclusions**

Who are we?

NetworksAndSecurity.Informatics (nas.inf)

- A dozen people's task force atm
- Research lines: automotive, IoT, VPAs fuzzing, human factor, semantic representation, threat modelling, formal methods
- Events:
  - Computer Security @ ACM Symposium on Applied Computing (SEC@SAC), since 2002
  - Workshop on Socio-Technical Aspects in SecuriTy (STAST), since 2011
  - Hardening hackathon since 2015
- Projects: EU NGI COSCA, EU NGI POC4COMMERCE, IT PRIN FuSeCar

The group is led by Prof. Giampaolo Bella https://www.dmi.unict.it/giamp/

NetworksAndSecurity.Informatics (nas.inf)

- Cybersec compliance methods and paths
- Offensive security activities
- Virtually in every area e.g.
  - **Metalworking** - Teksid, Comau
  - **Energy** - Axpo Group, Eviva Energia
  - **Data** - Cerved Group, Engineering Ingegneria Informatica, Expert IA, Metasystem
  - **Healthcare** - Gruppo San Donato, Fatebenefratelli
  - **Tech** - Unieuro, Samsung Italia
  - **Fashion** - LiuJo, Brunello Cucinelli
  - **Sector Associations**: OCF, Consulcesi
  - **Insurance**: Assimoco, Sara, Cattolica

Agenda

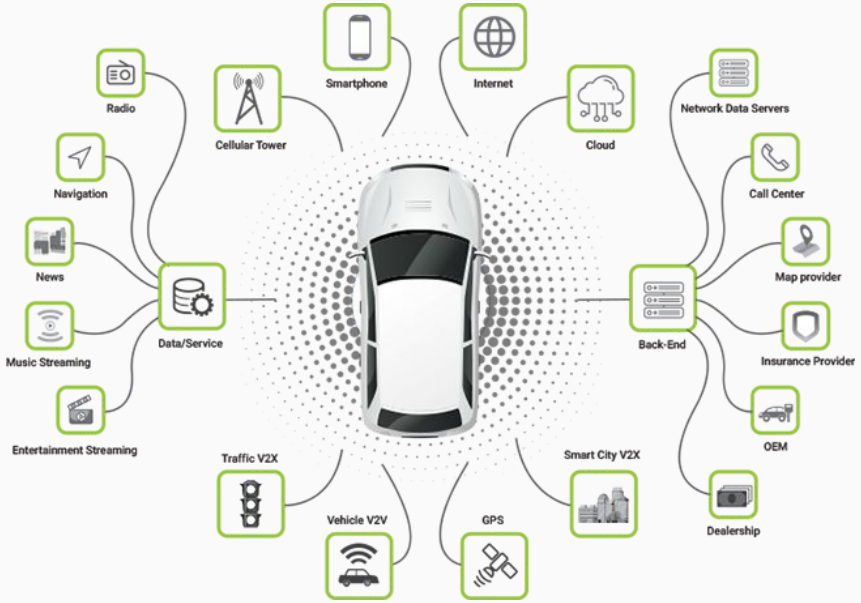
1. **Introduction**
2. SPADA for Privacy Threat Modelling
3. Demonstration on Smart Cars
4. Conclusions

Privacy may be summarised as “the right of the data subject to control or influence what information related to them may be collected, processed and stored, and by whom and to whom that information may be disclosed.”

- GDPR Interpretation

Privacy Threats in Automotive

Citizens' privacy is particularly threatened when people generate personal data by driving modern cars as well as by surfing the Internet.

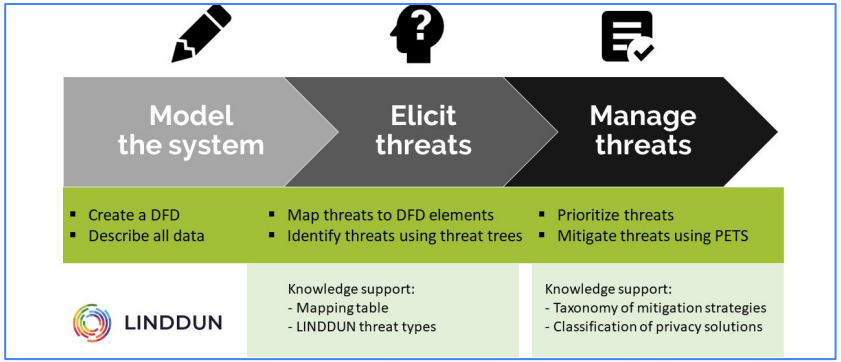


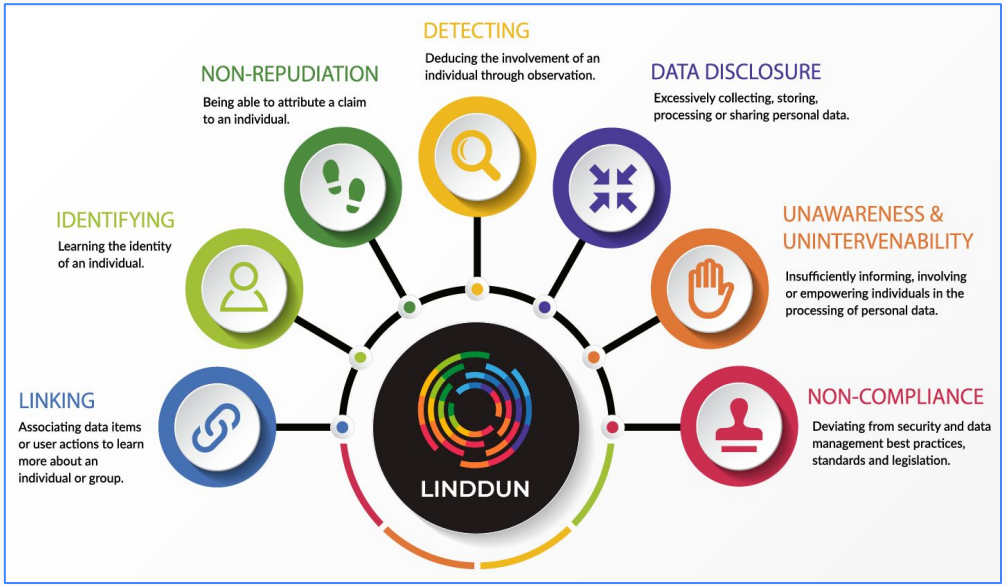
“**Threat modelling** works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.”

- OWASP

Privacy Threat Modelling with LINDDUN

LINDDUN is a privacy threat modelling methodology that supports analysts in systematically eliciting and mitigating privacy threats in software architectures.





Hard Privacy vs Soft Privacy

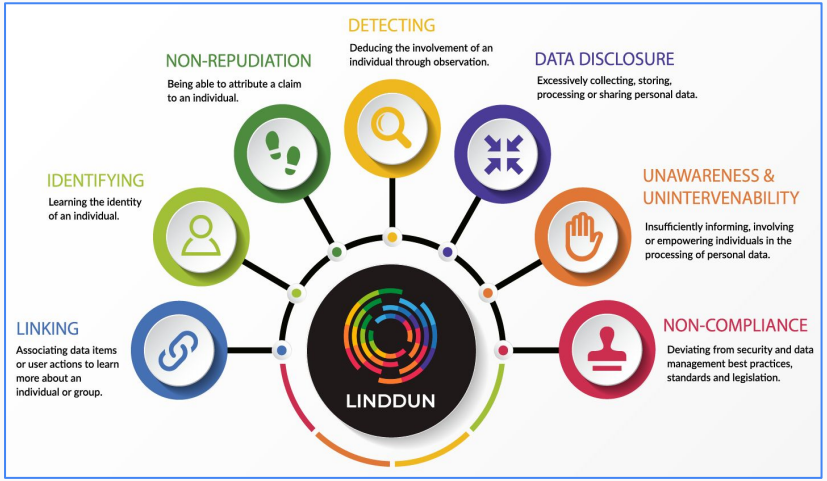
Hard Privacy:

Focus on minimising the risks associated with the collection and retention of personal data.

Soft Privacy:

Focus on the appropriate use and sharing of personal data while respecting individuals' rights to control their data.

L-I-N-D



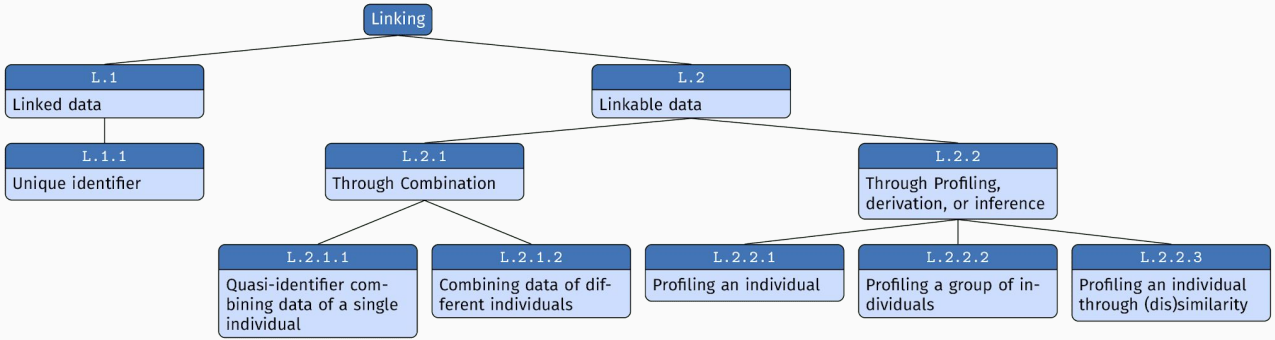
U-N

LINDDUN Knowledge Base

LINDDUN provides a set of threats specific to privacy, named as **“threat catalogue”**, in the form of threat trees.

The root node represents the ultimate goal.

The children nodes embody different ways of achieving that goal.



Agenda

1. Introduction
2. **SPADA for Privacy Threat Modelling**
3. Demonstration on Smart Cars
4. Conclusions

Privacy Threat Modelling Ingredients

Source of Documentation

> Internal
> External
> Hybrid

It provides the means to keep track of the version of the threats, e.g., the year in which the specific threat list is published.

Property within Privacy

> Hard Privacy
> Soft Privacy
> Cybersecurity

Cybersecurity plays a complementary role in terms of protection against the unauthorised access of data.

Application Domain

> Domain-Dependent
> Domain-Independent

A combination of the two approaches may offer a more effective and efficient analysis.

Detail (Level of)

> Hyponym/Meronym (higher / detailed)
> Hypernym/Holonym (lower / abstract)

A higher level of detail implies an estimation of the likelihood for a given threat with more precision.
The most appropriate level of detail should be considered within the main picture.

Agent(s) raising Threats

> Attacker
> Data processor
> Data controller
> Third party

TAs may also be considered in combination.

The Steps in SPADA

Step 0 — Variable Setup: consists in the choice of the five variables as the initial source of information that is employed in the subsequent steps.

Step 1 — Domain-Independent Threat Elicitation: involves the collection of the threats that the analyst deems relevant.

Step 2 — Domain-Dependent Asset Collection: consists of the collection of a list of assets for the target domain from relevant sources.

Step 3 — Domain-Dependent Threat Elicitation: produces a list of domain-specific threats.

The Steps in SPADA

Step 0 — Variable Setup: consists in the choice of the five variables as the initial source of information that is employed in the subsequent steps.

Step 1 — Domain-Independent Threat Elicitation: involves the collection of the threats that the analyst deems relevant.

Step 2 — Domain-Dependent Asset Collection: consists of the collection of a list of assets for the target domain from relevant sources.

Step 3 — Domain-Dependent Threat Elicitation: produces a list of domain-specific threats.

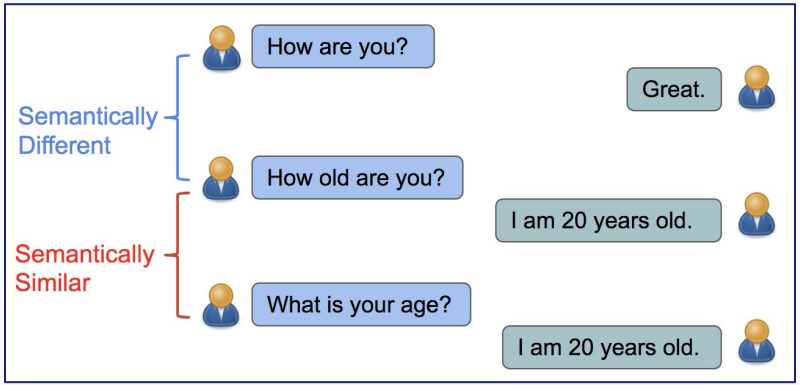
Embracing is adopted in Step 1 and Step 2 to achieve **completeness and avoid redundancy.**

Agenda

1. Introduction
2. **SPADA for Privacy Threat Modelling → Embracing**
3. Demonstration on Smart Cars
4. Conclusions

The Concept of Embracing

The concept of **embracing** wants to capture the standard scrutiny that the analyst operates in front of a list of threats/assets to understand the extent of their **semantic similarity**.



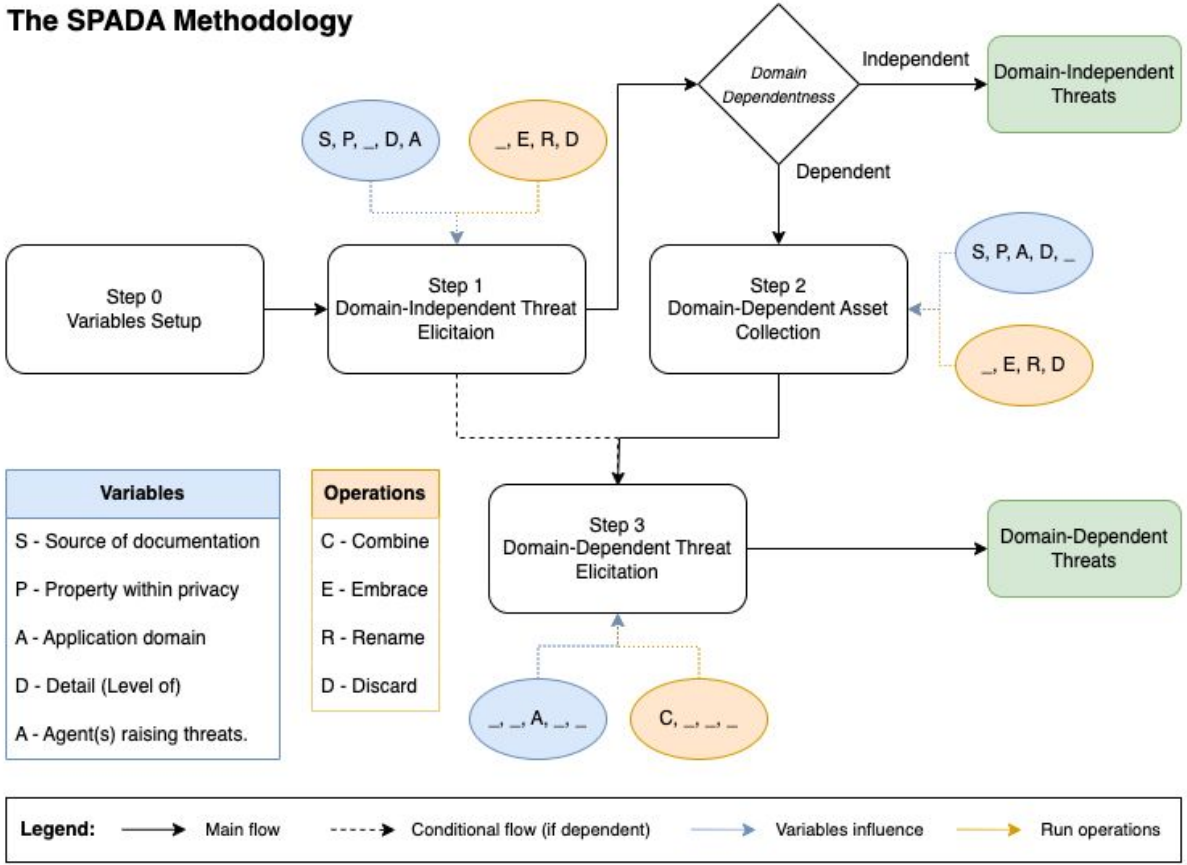
The Concept of Embracing

Elements of scrutiny derive from:

- the use of **synonyms** (e.g., “protocol” and “distributed algorithm”).
- the **level of detail** (e.g., “Unchanged default password” and “Human error”).

The analyst would conclude whether these threats/assets are *embraceable* and embrace them by selecting the one with an appropriate wording/level of detail, and discarding the other one.

Lost in all these details?


The SPADA Methodology
Domain Dependentness
Independent
Domain-Independent Threats
Dependent
S, P, _, D, A
_, E, R, D
Step 0
Variables Setup
Step 1
Domain-Independent Threat Elicitaion
Step 2
Domain-Dependent Asset Collection
S, P, A, D, _
_, E, R, D
Variables
S - Source of documentation
P - Property within privacy
A - Application domain
D - Detail (Level of)
A - Agent(s) raising threats.
Operations
C - Combine
E - Embrace
R - Rename
D - Discard
Step 3
Domain-Dependent Threat Elicitation
Domain-Dependent Threats
_, _, A, _, _
C, _, _, _
Legend:
Main flow
Conditional flow (if dependent)
Variables influence
Run operations

Agenda

1. Introduction
2. Privacy Threat Modelling Methodology
3. **Demonstration on Smart Cars**
4. Conclusions

Automotive Demo

Soft Privacy

Domain-dependent

External

Attacker, Data processor/controller, Third party

Abstract

Automotive Demo – Step 1

We selected a total of **23 privacy threats** from:

"Threat Catalogue Trees" (LINDDUN)

"Threat Taxonomy v2016" (ENISA)

"Good practices for security of smart cars" (ENISA)

"Calculation of the complete Privacy Risks list v2.0" (OWASP)

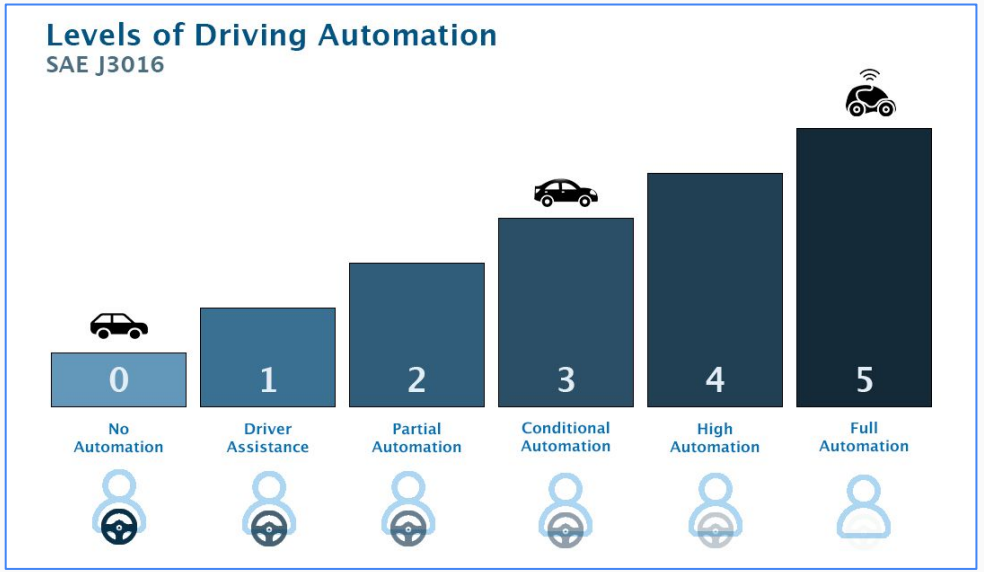
S	Threat
U	Unawareness of processing
	Unawareness as data subject
	Unawareness as a user sharing personal data
	Lack of data subject control
	Lack of data subject control – Preferences
	Lack of data subject control – Access
	Lack of data subject control – Rectification/erasure
N	Regulatory non-compliance
	GDPR
	Insufficient data subject controls
	Violation of data minimization principle
	Unlawful processing of personal data
	Invalid consent
	Lawfulness problems not related to consent
	Violation of storage limitation principle
	Improper personal data management
	Insufficient cybersecurity risk management
ENISA	Failure to meet contractual requirements
	Unauthorized use of IPR protected resources
	Judiciary decisions/court orders
OWASP	Misleading content
	Secondary use
	Sharing, transfer or processing through 3rd party

Automotive Demo – Step 2

We selected a total of **43 assets** from:

“Good practices for security of smart cars” (ENISA)

“A double assessment of privacy risks aboard top-selling cars” (Bella et al.)



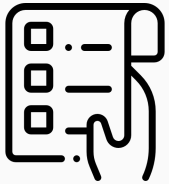
Automotive Demo – Step 3

S	Threat	Assets
U	Unawareness of processing	Sensors data, Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Unawareness as data subject	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Unawareness as a user sharing personal data	User information, Special categories of personal data
	Lack of data subject control	Map data, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Lack of data subject control - Preferences	User preferences, Purchase information
	Lack of data subject control - Access	User information, Special categories of personal data
	Lack of data subject control - Rectification/erasure	Sensors data, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
N	Regulatory non-compliance	All assets
	GDPR	All assets
	Insufficient data subject controls	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Violation of data minimization principle	Sensors data, Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Unlawful processing of personal data	All assets
	Invalid consent	All assets
	Lawfulness problems not related to consent	All assets
	Violation of storage limitation principle	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information, Vehicle information, Vehicle maintenance data
	Improper personal data management	User information, Special categories of personal data
	Insufficient cybersecurity risk management	All assets
ENISA	Failure to meet contractual requirements	All assets
	Unauthorized use of IPR protected resources	All assets
	Judiciary decisions/court orders	All assets
OWASP	Misleading content	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences
	Secondary use	All assets
	Sharing, transfer or processing through 3rd party	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information, Vehicle information, Vehicle maintenance data

Automotive Demo – Results

> **23 soft privacy threats**

> **43 assets**



These soft privacy threats are both *domain-independent* and *domain-dependent*.
(by appropriate combinations, we obtain 525 automotive-specific threats)

Agenda

1. Introduction
2. Privacy Threat Modelling Methodology
3. **Demonstration on Smart Cars → Case Study**
4. Conclusions

Technology

Toyota's Indian unit warns of a possible customer data breach

Reuters

January 3, 2023 9:41 PM GMT+1 · Updated 6 months ago

A Toyota Logo is seen at a Toyota dealership in Zaventem, Belgium, November 25, 2022. REUTERS/Johanna Geron/

Jan 1 (Reuters) - A data breach at Toyota Motor's (7203.T) Indian business might have exposed some customers' personal information, it said on Sunday.

Reviews

The Ring Car Cam takes Ring's great security smarts on the road

Jason Cipriani, CNN Underscored

Updated 11:08 AM EST, Thu February 16, 2023

Jason Cipriani

February 22, 2023 08:09 AM

Tesla escapes fine from Dutch watchdog after automaker alters security cameras

Tesla made changes to its "Sentry Mode" that include warning passers by of its activation and requiring approval from the car's owners in order to begin filming.

Reuters

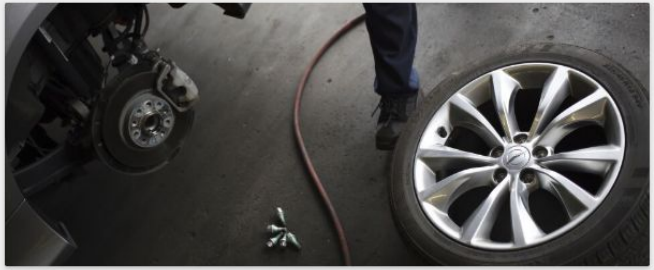
Some matching threats:

Insufficient data subject control

Violation of data minimization principle

Judiciary decisions/court order

Privacy & Data Security Law



The National Highway Traffic Safety Administration advised Massachusetts automakers to buck the state's "right to repair" law, which requires giving third parties open remote access to vehicles' telematics data. Photographer: Luke Sharrett/Bloomberg

June 15, 2023, 11:05 AM GMT+2

New US Agency Joins Fray Over Massachusetts Repair Law, Car Data

Skye Witley
Reporter

Listen

- 'Right to repair' compels automakers to allow remote access
- Traffic safety agency warns of dangers, says law is preempted

BMW exposes clients in Italy

Updated on: 10 March 2023

Jurgita Lapienytė, Chief Editor

Shutterstock/Cybernews

Hackers have been enjoying their fair share of the spotlight by breaching car manufacturers' defenses. The latest Cybernews discovery showcases that popular car brands sometimes leave their doors open, as if inviting threat actors to feast on their client data.

Some matching threats:

Insufficient cybersecurity risk management

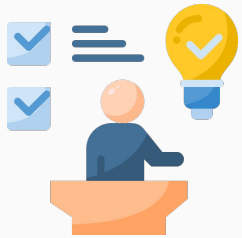
Judiciary decisions/court order

Agenda

1. Introduction
2. SPADA for Privacy Threat Modelling
3. Demonstration on Smart Cars
4. **Conclusions**

Conclusions

The risks for “*natural persons with regard to the processing of personal data and on the free movement of such data*” can be now assessed more precisely, especially if those natural persons drive **smart cars**.



Future work includes:

- *deeper semantic analysis (semantic relations for the level of detail)*
- *automation of embracing*

References

Bella G., Biondi P. and Tudisco G. (2023). A Double Assessment of Privacy Risks Aboard Top-Selling Cars. Springer Automotive Innovation 6, 146–163 (2023). DOI: 10.1007/s42154-022-00203-2

Raciti M. and Bella G. (2023). How to Model Privacy Threats in the Automotive Domain. In Proceedings of the 9th International Conference on Vehicle Technology and Intelligent Transport Systems - VEHITS; ISBN 978-989-758-652-1; ISSN 2184-495X, SciTePress, pages 394-401. DOI: 10.5220/0011998800003479

Raciti M. and Bella G.(2023). A Threat Model for Soft Privacy on Smart Cars. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Delft, Netherlands, 2023, pp. 1-10. DOI: 10.1109/EuroSPW59978.2023.00005.

Raciti M. and Bella G. (In press.). Up-to-date Threat Modelling for Soft Privacy on Smart Cars. In 7th International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2023). DOI: 10.48550/arXiv.2308.11273

Thanks for your attention!

For more information or questions:

giamp@dmi.unict.it – mario.raciti@imtlucca.it

dmi.unict.it/giamp/ - tsumarios.github.io/

@nassecuritynews - @tsumarios

Giampaolo Bella - Mario Raciti

NaS.Inf
nas.dmi.unict.it