A Threat Model for Soft Privacy on Smart Cars

Mario Raciti and Giampaolo Bella

ACSW'23

03/07/23 – Delft

Agenda

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

Agenda

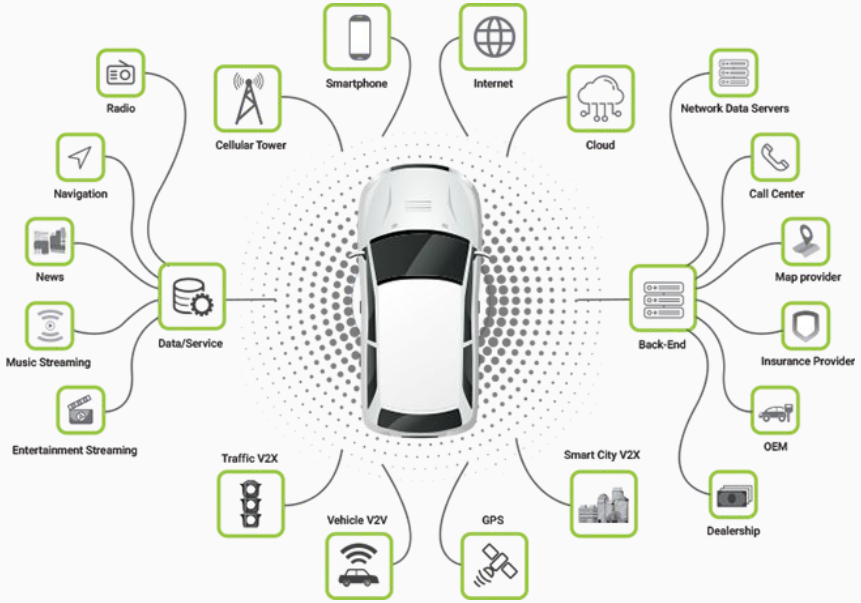
1. **Introduction**
2. Privacy Threat Modelling Methodology
3. Demonstration on Smart Cars
4. Conclusions

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.

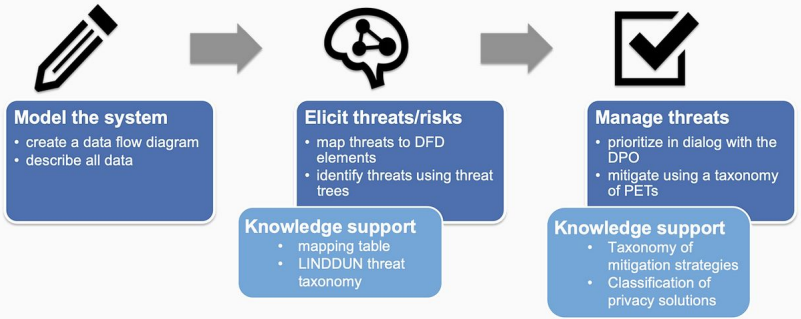


“**Threat modelling** works to identify, communicate, and understand threats and mitigations within the context of protecting something of value.”

- 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.



Linkability
An adversary is able to link two items of interest without knowing the identity of the data subject(s) involved.

Identifiability
An adversary is able to identify a data subject from a set of data subjects through an item of interest.

Non-repudiation
The data subject is unable to deny a claim (e.g., having performed an action, or sent a request).

Detectability
An adversary is able to distinguish whether an item of interest about a data subject exists or not, regardless of being able to read the contents itself.

Disclosure of information
An adversary is able to learn the content of an item of interest about a data subject.

Unawareness
The data subject is unaware of the collection, processing, storage, or sharing activities (and corresponding purposes) of the data subject's personal data.

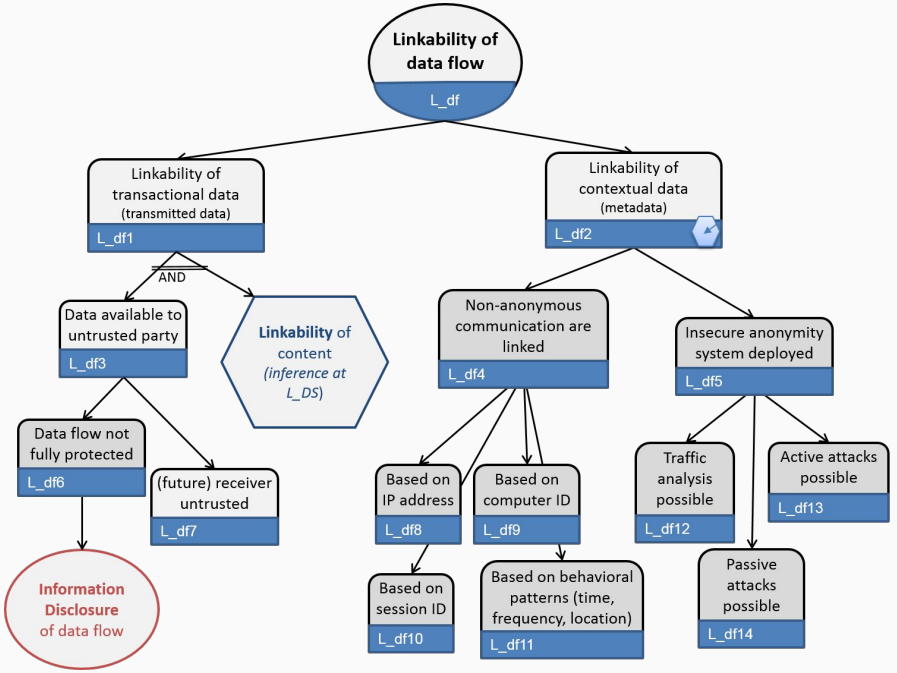
Non-compliance
The processing, storage, or handling of personal data is not compliant with legislation, regulation, and/or policy.

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.



Hard Privacy vs Soft Privacy

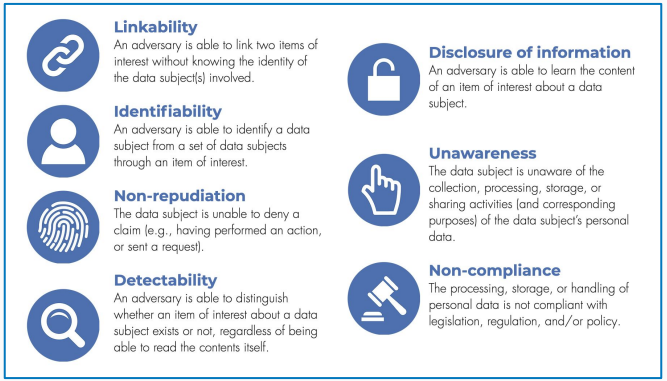
Hard Privacy:

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

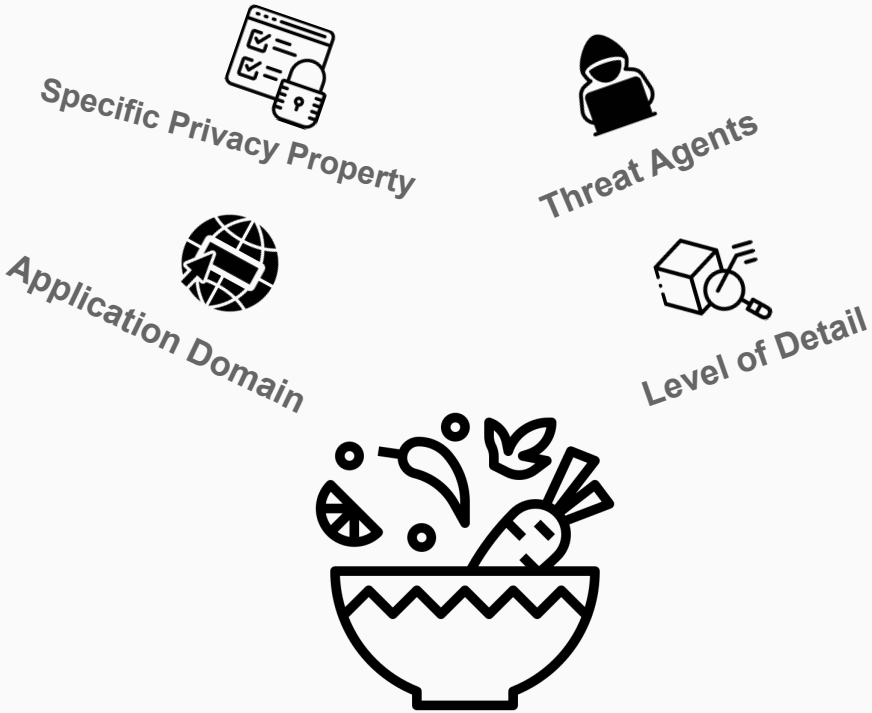


U-N

Agenda

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

Privacy Threat Modelling Ingredients



Specific Privacy Property

> Hard Privacy
> Soft Privacy
> Cybersecurity

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

Threat Agents

> Attacker
> Data processor
> Data controller
> Third party

TAs may also be considered in combination.

Application Domain

> Domain-Dependent
> Domain-Independent

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

Level of Detail

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

A hyponym implies a more precise likelihood estimation. However, an excessive level of detail leads to an exact assignment of the likelihood (either the bottom or the top value).

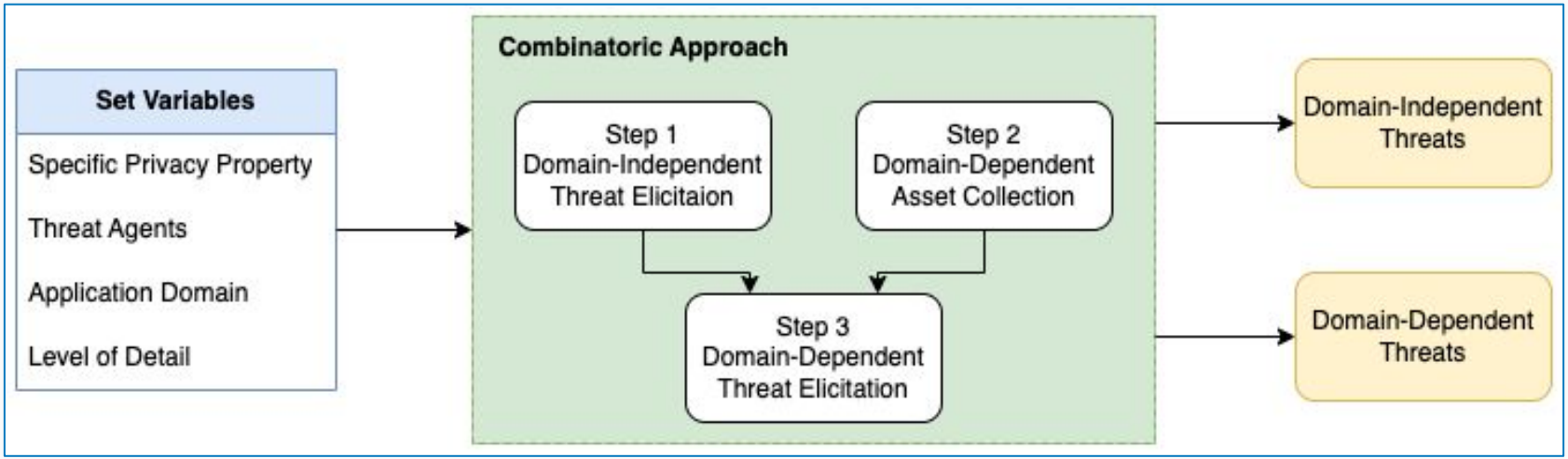
Combinatoric Approach

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.

Privacy Threat Modelling Methodology



Agenda

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

Automotive Demo

Soft Privacy

Domain-dependent

Attacker, Data processor/controller, Third party

Abstract (Hypernym)

Automotive Demo – Step 1

We selected a total of **17 privacy threats** from:

"Threat Catalogue Trees" (LINDDUN)

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

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

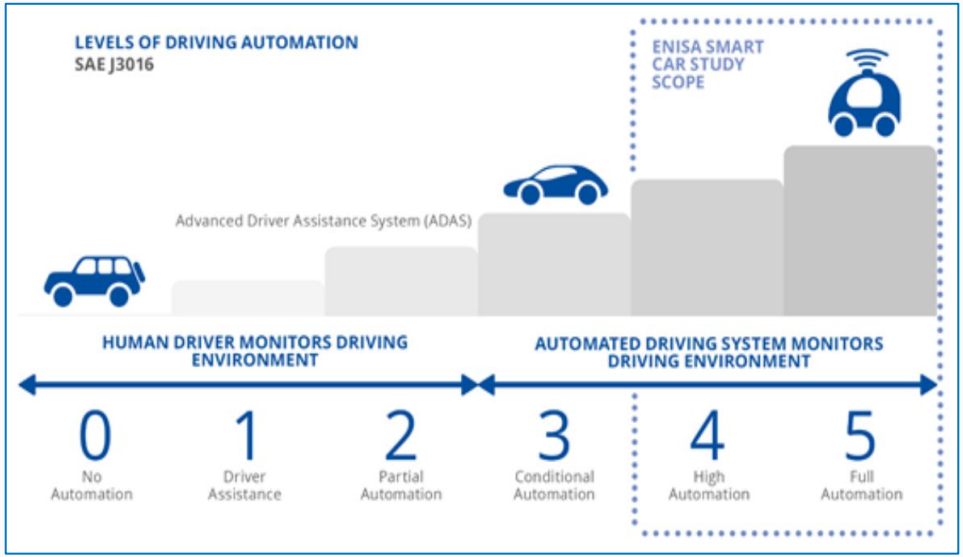
Source	Threat
U	Providing too much personal data
	Unaware of stored data
	No/insufficient feedback and awareness tools
	No user-friendly privacy support
	Unable to review personal information (data accuracy)
N	Attacker tampering with privacy policies and makes consents inconsistent
	Incorrect or insufficient privacy policies
	Inconsistent/insufficient policy management
	Insufficient notice
ENISA	Failure to meet contractual requirements
	Violation of rules and regulations/Breach of legislation/ Abuse of personal
OWASP	Consent-related issues
	Inability of user to access and modify data
	Insufficient data breach response
	Misleading content
	Secondary use
	Sharing, transfer or processing through 3rd party

Automotive Demo – Step 2

We selected a total of **41 assets** from:

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

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



Source: ENISA

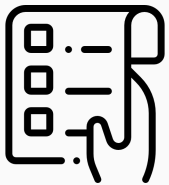
Automotive Demo – Step 3

Source	Threat	Assets
U	Providing too much personal data	User information, Special categories of personal data
	Unaware of stored data	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	No/insufficient feedback and awareness tools	Map data, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information
	No user-friendly privacy support	Sensors data, Map data, V2X information, Device information, User information, Special categories of personal data, Driver's behaviour, User preferences, Purchase information
	Unable to review personal information (data accuracy)	User information, Special categories of personal data
N	Attacker tampering with privacy policies and makes consents inconsistent	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
	Incorrect or insufficient privacy policies	All assets
	Inconsistent/insufficient policy management	All assets
	Insufficient notice	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data
ENISA	Failure to meet contractual requirements	All assets
	Violation of rules and regulations/Breach of legislation/ Abuse of personal data	All assets
OWASP	Consent-related issues	All assets
	Inability of user to access and modify data	Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	Insufficient data breach response	Sensors data, Key and certificates, Map data, V2X information, Device information, User information, Special categories of personal data, User preferences, Purchase information
	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

Automotive Demo – Results

The full outcomes include **17 soft privacy threats**.

These threats are both *domain-independent* and *domain-dependent (automotive)*.



Case Study

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 breach response

Violation of rules and regulations/Breach of legislation/Abuse of personal data

No user-friendly privacy support

Agenda

1. Introduction
2. Privacy Threat Modelling Methodology
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)*
- *application to different tuple of variables (e.g., hard privacy, high level of detail)*

Thanks for your attention!

For more information or questions:

mario.raciti@imtlucca.it – mario.raciti@phd.unict.it

https://tsumarios.github.io/

@tsumarios

https://linkedin.com/in/marioraciti

Non-malicious QR (maybe)