Privacy-enhancing threat analysis and risk assessment for connected and automated vehicles

Benyahya, Meriem; Lenard, Teri; Collen, Anastasija; Nijdam, Niels Alexander

The 23rd Privacy Enhancing Technologies Symposium

July 10-15, 2023 Lausanne, Switzerland

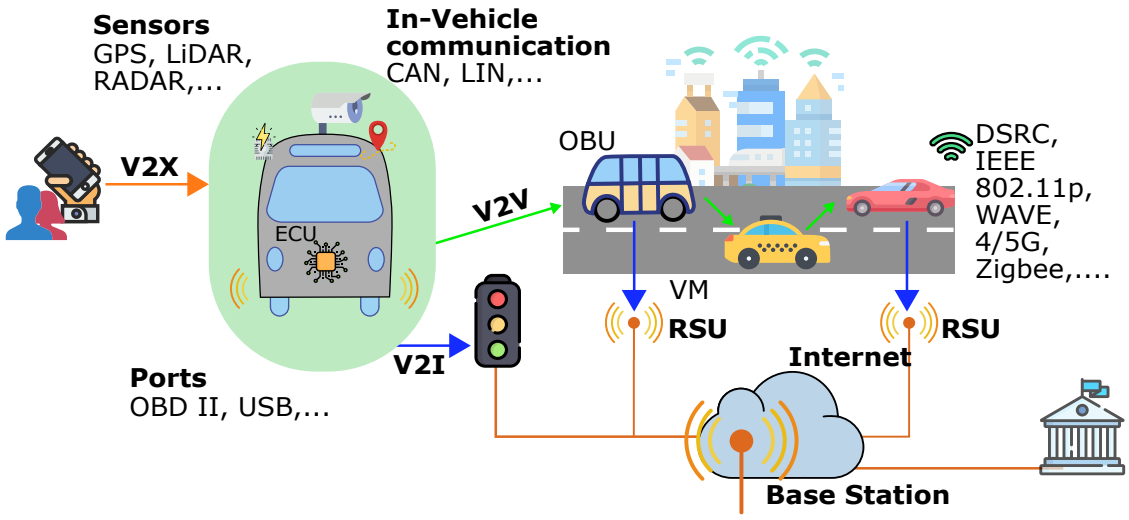
Privacy-Enhancing Threat Analysis and Risk Assessment for Connected and Automated Vehicles

Background

CAVs' cutting edge technologies represent advantageous conditions for cyber attacks and data breaches.

Personal Identifiable Information (PII) data is likely to be collected and processed (eg route taken, stop points) in the CAV's environment.

TARA was manadated by ISO/SAE 21434 and UNECE R155 to ensure acceptable level of risk with regard to cybersecurity requirements.



Problem

Privacy threats and their related impacts are not adequatly addressed in TARA.

Threat scenarios are derived using STRIDE but not based on a privacy oriented threat modeling tool.

Unlike safety and financial impacts, privacy and operations impacts are underestimated:

$$i_{sum} = 10(i_s + i_f) + i_o + i_p$$

Methods

Identifying improvement avenues for a granular privacy assessment.

Extending CIA properties to include privacy goals.

Associating STRIDE and LINDDUN threat classes to the GDPR for threat scenarios identification.

Enhancing the privacy impact by assigning a weight reflecting data sensitivity, linkability and the mitigation techniques in place.

Future Orientations

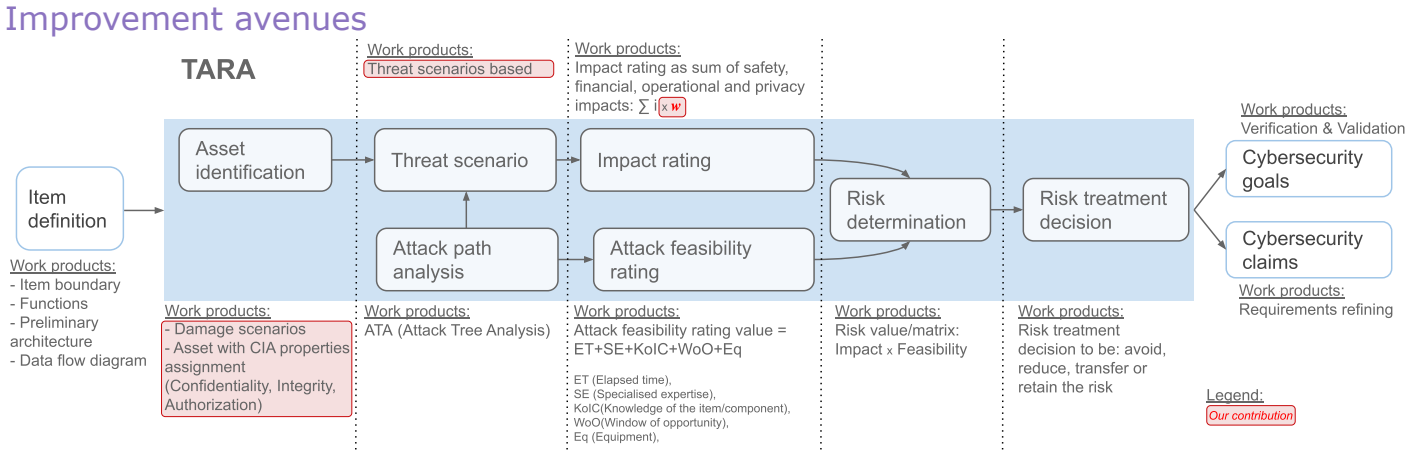
Analyse the relationship between the privacy risks evolvment and the vehicle SAE level.

Define a computation method for Privacy Assurance Level (PAL) similar to the Cybersecurity Assurance Level (CAL) but dedicated to data privacy.

Consider privacy threats in assessing the residual risk (the risk of unknown threats) within the TARA process.

Results

Improvement avenues



Extended CIA triad properties

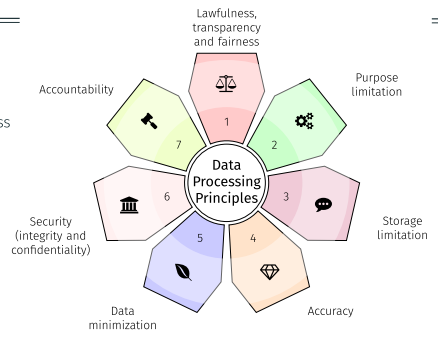
For ganular analysis of the damage scenarios, the ISO 27000 CIA triad is extended to consider:
(i) identification tracking and profiling attacks,
(ii) system or data users' responsabilities and
(iii) overall compliance to GDPR or other legislations.

Security goals	Designation	Description
Confidentiality	C	Assuring that information is accessed only by authorized users
Integrity	I	Ensuring that information is accurate and complete
Availability	A	Making data accessible when needed by authorized users
Unlikability	U	Protecting from associating an identifier or a pseudonym with an individual
Accountability	Ac	Assuring that actions can be traced back to a specific individual
Compliance	Com	Achieving an alignment with the GDPR data processing principles

Merging STRIDE & LINDDUN to GDPR for an improved threat modelling

STRIDE	Security goal	GDPR principle
Spoofing	A	Security
Tampering	I	Security
Repudation	Ac	Accountability
Information disclosure	C	Security
Denial-of-service	A	Lawfulness, transparency and fairness

(+) automated tool for security threats modelling
(–) not adapted to data privacy threats



LINDDUN	Security goal	GDPR principle
Linkability	U	Data minimization
Identifiability	U	Data minimization
Non-repudation	Ac	Accountability
Detectability	Ac	Accountability
Disclosure of information	C	Security
Unawareness	A	Lawfulness, transparency and fairness
Non-compliance	Com	Lawfulness, transparency and fairness

(+) focused on privacy threats
(–) does not address all GDPR requirements

Privacy enhacement within the impact rating

Sensitivity	Privacy impact (i_p) Linkability to PII	Privacy-preserving	Value (V)	Weight (w_p)
High	High	None	100	10
High	High	Yes	10	5
Medium	High	Yes	10	5
High	Medium	Yes	10	5
Medium	Medium	None	10	5
Medium	Medium	Yes	1	2
Not sensitive	Easy to link	None	1	2
Sensitive	Difficult to link	None	1	2
Not sensitive	Difficult to link	Yes	1	1
Not sensitive	Difficult to link	None	0	1

$$i_p = V * w_p$$

$$i_{sum} = \sum_{j \in \{s,f,o,p\}} w_{i,j} i_j$$

Impact sum (i_{sum})	Impact level
0	0 - none
1-19	1 - negligible
20-99	2 - moderate
100-999	3 - major
≥ 1000	4 - severe

Based on a refinement of the ISO/IEC 29100, the privacy impact is analysed to reflect data sensitivity, linkability and the deployed mitigation techniques.

To compute the privacy impact, a privacy weight is associated to the impact value.

The impact level is derived from the impact sum wrapping up the safety, financial, operational and privacy impact.

ULTIMO project
https:https://ultimo-he.eu/
Grant agreement No 101077587

SHOW project
https://show-project.eu/
Grant agreement No 875530

Co-funded by the European Union

Project funded by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

References

- Giampaolo Bella, Pietro Biondi, and Giuseppe Tudisco. A Double Assessment of Privacy Risks Aboard Top-Selling Cars. Automotive Innovation, 2023.
- N. Azam, L. Michala, S. Ansari, and N. B. Truong, "Data Privacy Threat Modelling for Autonomous Systems: A Survey from the GDPR Perspective," IEEE Transactions on Big Data, 4 2022.
- Meriem Benyahya, AnastasijaCollen,Sotiria Kechagia,and NielsAlexanderNijdam. 2022. Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments. Computers & Security 122 (11 2022), 102904. https://doi.org/10.1016/j.cose.2022.102904
- Meriem Benyahya, Sotiria Kechagia, Anastasija Collen, and Niels Alexander Nijdam. 2022. The Interface of Privacy and Data Security in Automated City Shuttles: The GDPR Analysis. Applied Sciences 12, 9 (4 2022), 4413. https: //doi.org/10.3390/app12094413
- Meriem Benyahya, Pierre Bergerat, Anastasija Collen, and Niels Alexander Nijdam. Symbiotic Analysis of Security As- sessment and Penetration Tests Guiding Real L4 Automated City Shuttles. Telecom, 4(1):198–218, 3 2023.
- ISO. ISO/SAE 21434 Road vehicles-Cybersecurity engineering. Technical report, ISO/SAE, 8 2021.
- UNECE. 2020. R155. Technical Report. UNECE. 1–194 pages.

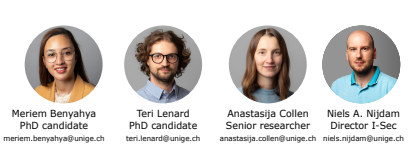
Icons from https://www.flaticon.com/packs

Acronyms

CAV: Connected and Automated Vehicles
ISO: International Organization for Standardization
LINDDUN: Linkability, Identifiability, Nonrepudiation, Detectability, Disclosure of data, Unawareness, and Noncompliance
PII:Personal Identifiable Information
SAE: Society of Automotive Engineering
STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service and Elevation of privilege
TARA:Threat Analysis and Risk Assessment
UNECE: United Nations Economic Commission for Europe

UNIVERSITÉ DE GENÈVE
GENEVA SCHOOL OF ECONOMICS AND MANAGEMENT
Institute of Information Service Science

Information Security Group


Meriem Benyahya
PhD candidate
meriem.benyahya@unige.ch
Teri Lenard
PhD candidate
teri.lenard@unige.ch
Anastasija Collen
Senior researcher
anastasija.collen@unige.ch
Niels A. Nijdam
Director I-Sec
niels.nijdam@unige.ch