Human-Artificial Intelligent Threat Modelling in the Automotive Domain

G. Bella, G. Castiglione, S. Esposito,
M.G. Mangano, G. Pampallona, **M. Raciti**,
S. Riccobene, D.F. Santamaria

IOLTS 2025

IMT SCHOOL FOR ADVANCED STUDIES LUCCA

Università di Catania

09/07/25 – Ischia, IT

It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy

By **Jen Caltrider, Misha Rykov** and **Zoë MacDonald** | Sept. 6, 2023

cybernews®

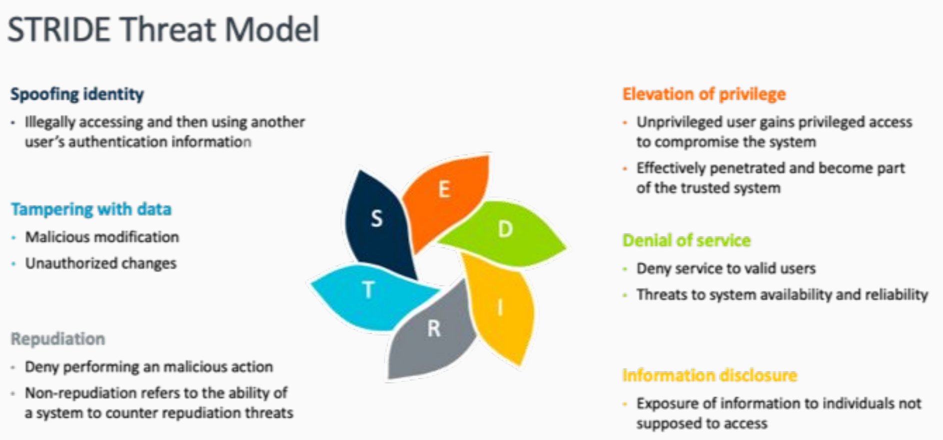
Home » Privacy

Smart cars vs. privacy: a driverless car could generate 100 GB of data per second

TC

Toyota Japan exposed millions of vehicles' location data for a decade

Related Work



Zero Trust, Pseudonymisation, Data Minimisation widely recognised as *foundational principles*

A Glimpse at SCAR4SUD

SCAR's Four Security-Unravelling Dimensions (SCAR4SUD)

SCAR4SUD

Objectives:

1 - Integrating multi-layered security and privacy engineering practices

2 - Defending by multi-layer measures, including hardware, software, and communication protocols

3 - Securing and protecting personal data in automotive

4 - Integrating multi-disciplinary approaches towards security and privacy

Gap and Contributions

Traditional **threat modelling** is often **manual** and **time-consuming**

Regulatory demands are increasing, especially for **modern systems** (*e.g., automotive*)

<u>Our work:</u>

Takes a *multi-level* **Human Artificial Intelligence (HAI)** approach through *four phases*

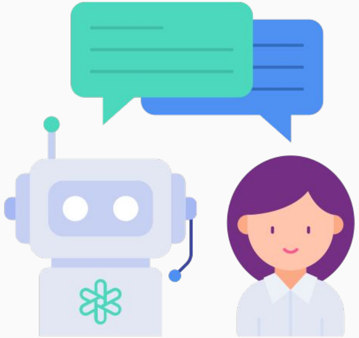
Ensures coverage of both **security and privacy threats** and their **mitigation**

Agenda

1. Introduction
2. **Methodology**
3. Augmented Mitigation Plan
4. Conclusions

Methodology in a Nutshell

Our methodology is **multi-level** because it involves a few **levels of refinement** of the target outputs *sequentially*



This implies **Human-Artificial Intelligence** *loop* in each phase

Each of the phases is executed using **different instantiations** of this *multi-level strategy*

Agenda

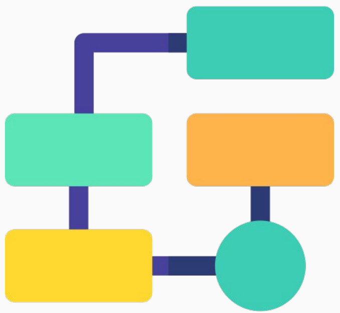
1. Introduction
2. **Methodology → Target System Modelling**
3. Partial Validation
4. Conclusions

Target System Modelling

The input is a *structured technical document* describing the **SCAR4SUD architecture**

(L1: AI) LLM parses the document and extracts diagrams in textual form

(L2: Human) Expert validation and refinement of the diagrams



The output is a *ground-truth system representation*

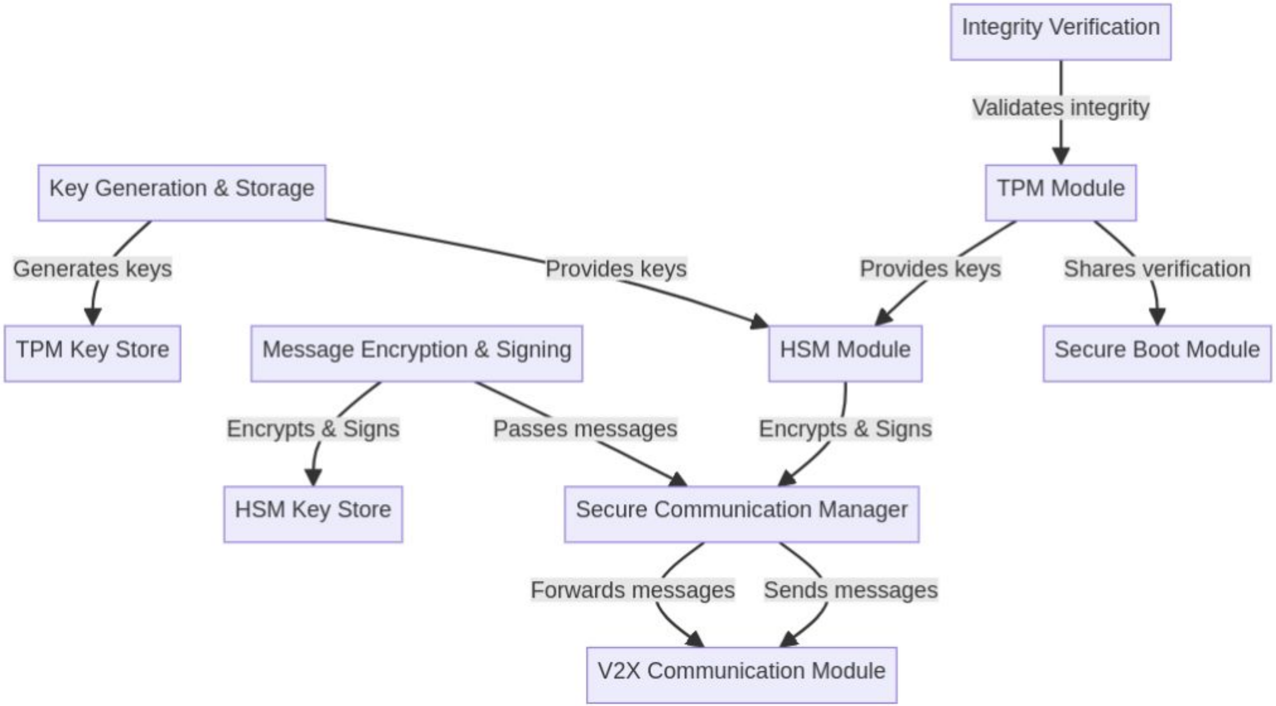


Figure 4: Data flow diagram of the target system.

Agenda

1. Introduction
2. **Methodology → Asset and Threat Elicitation**
3. Partial Validation
4. Conclusions

Asset Identification

We operate in a *three-level* style due to the need for **semantic grounding**

- **(L1: AI)** LLM generates the initial asset lists at an abstract level
- **(L2: Human)** Experts identify semantic relations for refinement
- **(L3: AI)** LLM few-shot prompting to regenerate enhanced results

Reflects an iterative abstraction-specialisation loop, guided by *taxonomic knowledge* and *controlled prompting*

Table 2: Security assets from L1 identification step

Asset	Brief description
Cryptographic Keys	Cryptographic material that is deemed to be kept secret
Device Identity	Identifiers of any electronic network component
Authentication Credentials	Credentials used to go through login
Secure Boot Measures	Information used to verify boot integrity
V2X Messages (Signed & Encrypted)	Signed/encrypted messages exchanged among vehicles
Secure Communication Channels	Links within the communication infrastructure
Middleware Interfaces	API-exposed services
Log Records	Log information supporting auditing processes
Key Management Infrastructure	Key lifecycle framework
RSU Trust Components	RSU-local functional elements

Table 3: Security assets from L2 identification step

Asset	Examples
Cryptographic Keys	Long-term keys, session keys, pseudonym keys
Device Identity	Device fingerprint id, (physical) mac address, device (private) key stored in the TPM
Authentication Credentials	Password, passkey, passphrase, key, token, OTP, wearable devices
Secure Boot Measures	Firmware signatures, Operating System signatures, hash values
V2X Messages (Signed & Encrypted)	Vehicle-to-vehicle communications, DSRC messages, WAVE messages, vehicle-to-infrastructure communications, vehicle-to-RSU communications
Secure Communication Channels	TLS channels, IPSec channels, IEEE 1609.2 channels
Middleware Interfaces	API keys, API interfaces, APIs, microservices, Model Context Protocol
Log Records	Access logs, command history logs, network logs, system logs, Operating System logs
Key Management Infrastructure	Public-key infrastructures, key stores, key rings, HSMs, TPMs, certificate authorities, certificates
RSU Trust Components	Failover mechanisms, edge computing modules, V2X sensors

Table 4: Security assets from L3 identification step

Asset	Specific assets
Cryptographic Keys	Long-term keys, session keys, pseudonym keys, pseudonym keys, group keys, pre-shared keys, KEKs, DEKs, attestation keys, update signing key, ephemeral Keys
Device Identity	Device fingerprint id, (physical) mac address, device (private) key stored in the TPM, VIN, hardware serial number, IMEI / eUICC, certificate thumbprint, software-defined identifier
Authentication Credentials	Password, passkey, passphrase, key, token, OTP, wearable devices
Secure Boot Measures	Firmware signatures, Operating System signatures, hash values
V2X Messages (Signed & Encrypted)	Vehicle-to-vehicle communications, DSRC messages, WAVE messages, vehicle-to-infrastructure communications, vehicle-to-RSU communications
Secure Communication Channels	TLS channels, IPSec channels, IEEE 1609.2 channels
Middleware Interfaces	API keys, API interfaces, APIs, microservices, Model Context Protocol
Log Records	Access logs, command history logs, network logs, system logs, Operating System logs
Key Management Infrastructure	Public-key infrastructures, key stores, key rings, HSMs, TPMs, certificate authorities, certificates
RSU Trust Components	Failover mechanisms, edge computing modules, V2X sensors, certificate validation engine, CRL caching & distribution, hardware root of trust (RoT), trusted time synchronization source, revocation enforcement mechanism

Threat Elicitation

Threats are generated using a similar approach

- **(L1: Human)** Experts apply STRIDE and LINDDUN to the initial asset lists
- **(L2: Human)** Experts apply STRIDE and LINDDUN to the specific assets
- **(L3: AI)** LLM generates a list of concrete instantiations of the threats

Table 8: Threat elicitation STRIDE at L1

Asset	S	T	R	I	D	E
Cryptographic Keys	✔	✔		✔		
Device Identity	✔	✔	✔	✔		✔
Authentication Credentials	✔	✔		✔		
Secure Boot Measures	✔	✔		✔		
V2X Messages (Signed & Encrypted)	✔	✔		✔		
Secure Communication Channels	✔	✔	✔	✔	✔	✔
Middleware Interfaces	✔	✔	✔	✔	✔	✔
Logging and Audit Records		✔	✔	✔		
Key Management Infrastructure	✔	✔	✔	✔	✔	✔
RSU Trust Components	✔	✔	✔	✔	✔	✔

Table 9: Threat elicitation LINDDUN at L1

Asset	L	I	N	D	D	U	N
Vehicle Identifiers	✔	✔	✔	✔			✔
Location Information	✔	✔	✔	✔	✔	✔	
Communication Metadata	✔	✔	✔	✔	✔	✔	
User Behavior & Preferences	✔	✔	✔	✔		✔	✔
Transmitted Message Content		✔		✔	✔	✔	
Log Data with Personal Context	✔	✔	✔	✔	✔	✔	✔
OTA Update Records					✔	✔	
Cloud-Linked Identifiers	✔	✔	✔	✔		✔	✔

Cryptographic Keys

- S1.1: Impersonation using stolen keys from a compromised TPM.
- S1.2: Use of leaked session keys to forge V2X messages.
- S1.3: Replay of signed messages using extracted keys.
- T1.1: Attacker modifies stored key material to alter message signing results.
- T1.2: Injection of unauthorised keys into HSM key store.
- T1.3: Manipulation of key lifecycle states (e.g., reuse of expired keys).
- I1.1: Side-channel attack (e.g., timing analysis) leaks key usage patterns.

...

Log Data with Personal Context

- L6.1: Same log token reused across user sessions.
- L6.2: Logs correlated across domains.
- L6.3: Debug logs link user identity and location.
- I6.1: Logs store identifiable queries.
- I6.2: Unencrypted log transfer reveals personal data.
- I6.3: Diagnostics leak user IDs to cloud.
- N6.1: Anonymized log lacks sender reference.
- N6.2: Logs modified without trace.
- N6.3: Deletion of key attribution fields.
- D6.1: RSU observer matches logs to vehicle.
- D6.2: Offline analysis links logs to driver.
- D6.3: Third-party access to raw logs.
- D6.4: Plaintext export of logged location.

Agenda

1. Introduction
2. **Methodology → Mitigation Plan**
3. Augmented Mitigation Plan
4. Conclusions

Mitigation Plan

The mitigation plan is obtained in a *two-level* fashion

- **(L1: AI)** LLM explores candidate mitigations with *ISO/IEC 27002 | GDPR* knowledge base
- **(L2: Human)** Experts refine the pairs threats-mitigations on system context and risk prioritisation

The output is a set of aligned **mitigations** covering both *security and privacy* threats

Table 12: Mitigation plan for STRIDE-identified Threats at L1-L2

Asset	S	T	R	I	D	E
Cryptographic Keys	sm1, sm2, sm3, sm12, sm24	sm2, sm3, sm9, sm15, sm24		sm2, sm7, sm11, sm12, sm23, sm24, sm25, sm28		
Device Identity	sm2, sm3, sm5, sm20	sm9, sm16, sm18	sm13, sm15, sm34	sm3, sm7, sm23, sm24		sm2, sm3, sm3, sm20
Authentication Credentials	sm2, sm3, sm5, sm12	sm9, sm15, sm16, sm18		sm3, sm5 sm7, sm12, sm24		
Secure Boot Measures	sm5, sm9, sm18, sm20, sm25, sm27	sm9, sm16, sm18, sm20, sm25, sm27		sm3, sm7, sm11, sm12, sm15, sm16, sm18, sm20, sm24		
V2X Messages (Signed & Encrypted)	sm3, sm5, sm20, sm24, sm25	sm9, sm12, sm16, sm24, sm25, sm27, sm32		sm3, sm7, sm11, sm12, sm15, sm16, sm24		
Secure Communication Channels	sm3, sm5, sm20, sm21, sm25, sm25	sm9, sm12, sm16, sm20, sm24, sm25, sm32	sm5, sm15, sm16, sm24, sm24	sm3, sm7, sm11, sm12, sm24	sm6, sm9, sm14, sm20	sm2, sm3, sm5, sm18
Middleware Interfaces	sm2, sm3, sm5, sm20, sm21, sm24, sm24	sm9, sm12, sm16, sm20, sm24, sm25	sm5, sm15, sm16, sm34	sm3, sm7, sm11, sm12, sm24	sm6, sm9, sm14, sm20	sm2, sm3, sm5, sm18
Logging and		sm9, sm15,	sm5, sm15,	sm3, sm11,		

Agenda

1. Introduction
2. Methodology
3. **Augmented Mitigation Plan**
4. Conclusions

Zoom in on Augmented Mitigation Plan

Verticalise **Zero Trust (ZT), Pseudonymisation (PS), Data Minimisation (DM)** to automotive

These principles are *mapped* over the previous mitigation plan

We proceed in a *two-level* fashion also in this case

(L1: Human) Experts assess and map ZT/PS/DM to the controls from relevant standards

(L2: AI) LLM confirms or perfects the mapping

Zero Trust in Automotive

NIST SP 800-207 meets vehicle as *mobile digital platform*

Interior: CAN / CAN FD, TSN Ethernet, ECUs

Exterior: OTA servers, mobile apps, V2X infrastructure

“Trust no bus, ECU or external endpoint”

Core Roles (verticalised):

PEP (vehicular gateway) enforces access rules on CAN / Ethernet

PDP (cloud) validates OTA updates, remote commands, data-access requests

PAP / Policy Engine orchestrate dynamic policies (e.g., driver identity, geolocation, SW version)

Pseudonymisation in Automotive

Asset-threat examples:

VIN → *fleet analytics*; **Driver ID** → *shared-mobility logs*; **GPS** → *route profiling*

Counter — ensures internal traceability without external linkage

RNG — can be used for synthetic datasets or simulation

Cryptographic hash — can provide a fixed-length, irreversible pseudonym

MAC — allows only authorised parties to derive or validate the pseudonym

Encryption — suitable for reversible pseudonymisation where re-identification is required

Data Minimisation in Automotive

Recognise data sources: identify which sensor/ECU streams are essential; discard non-critical data upstream

Apply selection and filtering logic: use local filtering, anonymisation, aggregation or deletion before telematics or app upload

Design data-aware architectures: ensure ECUs transmit only on-demand (e.g., throttle position sent only on diagnostic/error)

Separate technical data from personal information: send content metadata (e.g., media type) without user identity unless strictly required and consented

Handle GPS tracking with care: reduce transmission frequency or share derived context (e.g., “congested area”) instead of raw coordinates

Augmented Mitigation Plan Results

TABLE I
AUGMENTED MITIGATIONS FOR STRIDE-IDENTIFIED THREATS AT L1-L2

Asset	S	T	R	I	D	E
Cryptographic Keys	ZT, DM	ZT, DM		ZT, DM		
Device Identity	ZT, PS	ZT, PS	ZT, PS	ZT, PS		ZT, PS
Authentication Credentials	ZT, DM	ZT, DM		ZT, DM		
Secure Boot Measures	ZT, DM	ZT, DM		ZT, DM		
V2X Messages (Signed & Encrypted)	ZT, DM, PS	ZT, DM, PS		ZT, DM, PS		
Secure Communication Channels	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	-	ZT, DM, PS
Middleware Interfaces	ZT, DM	ZT, DM	ZT, DM	ZT, DM	-	ZT, DM
Logging and Audit Records		ZT, DM, PS	ZT, DM	ZT, DM		
Key Management Infrastructure	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	-	ZT, DM, PS
RSU Trust Components	ZT, DM, PS	ZT, DM	ZT, DM, PS	ZT, DM, PS	-	-

TABLE II
AUGMENTED MITIGATIONS FOR LINDDUN-IDENTIFIED THREATS AT L1-L2

Asset	L	I	N	D	D	U	N
Vehicle Identifiers	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS			ZT, DM, PS
Location Information	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM	
Communication Metadata	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM		
User Behavior & Preferences	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	-	ZT, DM, PS	ZT, DM, PS
Transmitted Message Content		ZT, DM, PS		ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	
Log Data with Personal Context	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM	ZT, DM
OTA Update Records					ZT, DM	ZT, DM	
Cloud-Linked Identifiers	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS	ZT, DM, PS		ZT, DM, PS	ZT, DM, PS

Takeaways

+ PS/DM selectively reinforce privacy controls

+ HAI loop improves both coverage and expert trust threats and their composition

- ZT is broadly applicable but not universal

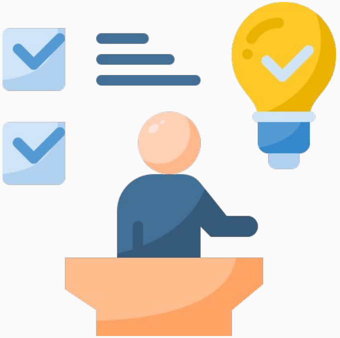
Agenda

1. Introduction
2. Methodology
3. Augmented Mitigation Plan
4. **Conclusions**

Conclusions

We presented a primer on the **SCAR4SUD Framework** for **security and privacy in the automotive domain**

It supports *security-and-privacy aware automotive architectures* rooted in **risk assessment** with a **multi-level HAI methodology**



Future work:

- Model assurance, explainability
- Adversarial robustness of the AI components

References

Project Website
https://scar4sud-project.dmi.unict.it/

https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model

https://linddun.org/

https://www.mozillafoundation.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

https://cybernews.com/privacy/smart-cars-vs-privacy-a-driverless-car-could-generate-100-gb-of-data-per-second/

https://techcrunch.com/2023/05/12/toyota-japan-exposed-millions-locations-videos/

Disclaimer: Icons in this presentation were obtained from www.flaticon.com

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)