HoliSec

Holistic Approach to Improve Data Security

State of the Art of Secure Vehicular Communication and Design

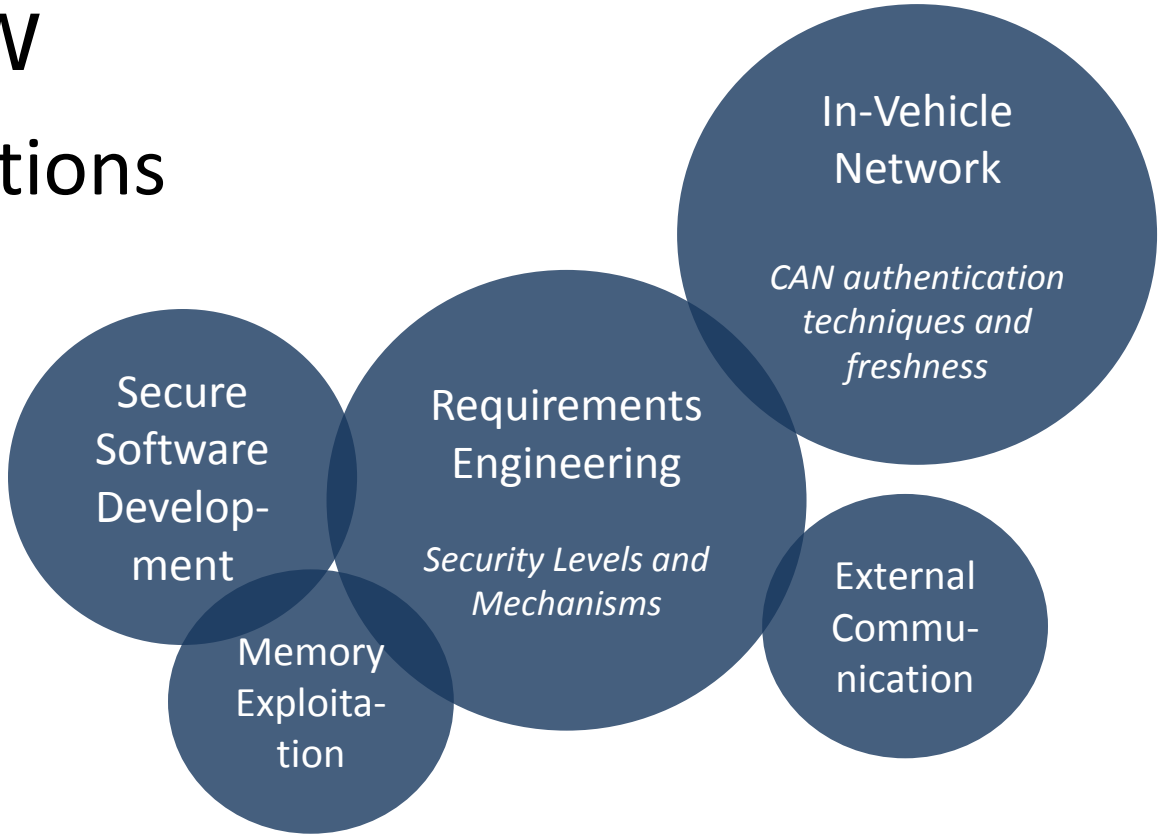
Presenters: Lautenbach, Nowdehi, Rosenstatter

March 26, 2019. Time 12:45 – 13:30

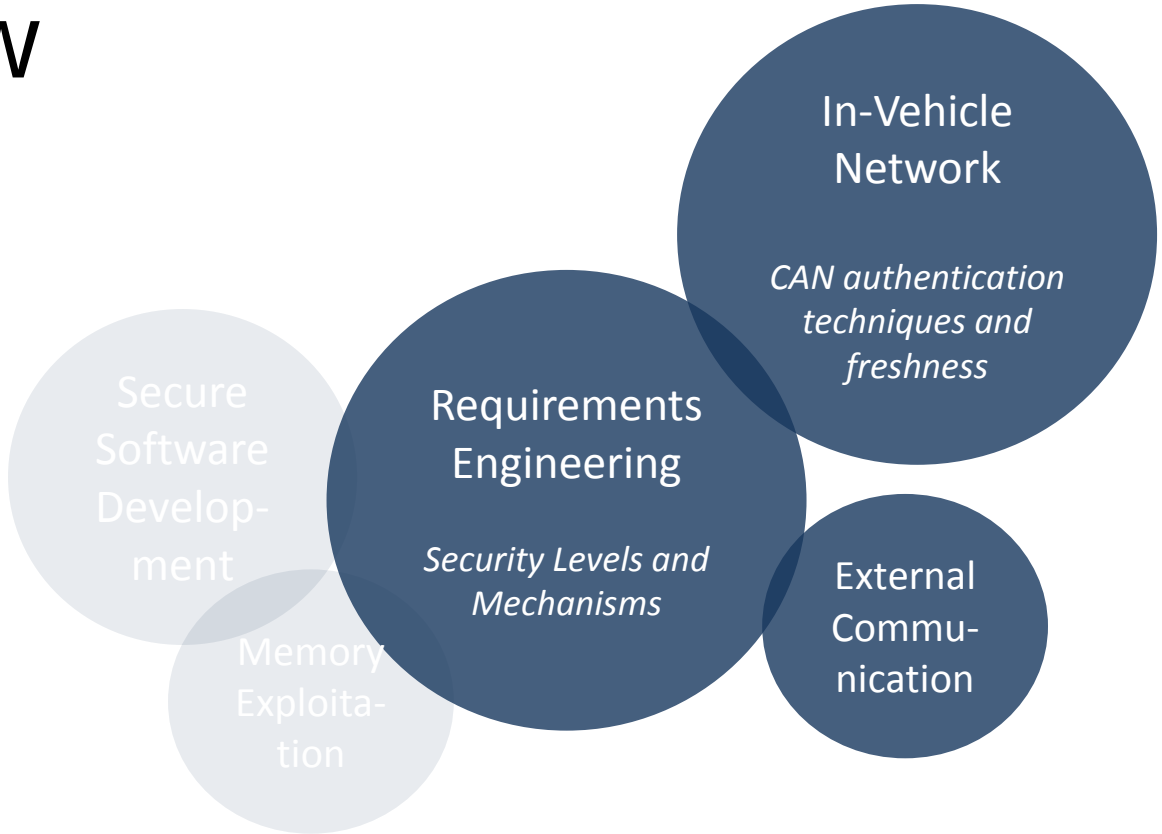
VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI. SE Research Institutes of Sweden

Overview

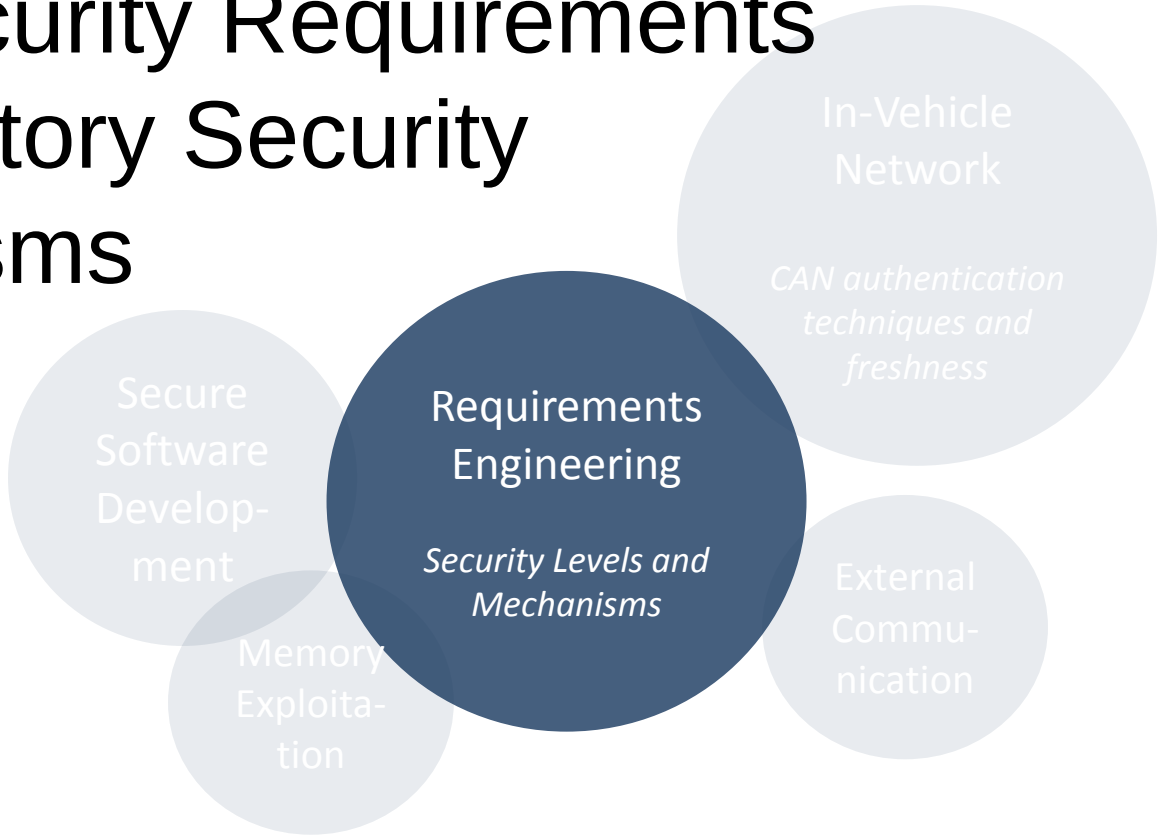
- 8 publications



Overview


In-Vehicle Network
CAN authentication techniques and freshness
Requirements Engineering
Security Levels and Mechanisms
External Commu-nication
Secure Software Develop-ment
Memory Exploita-tion

From Security Requirements to Mandatory Security Mechanisms



From Security Requirements to Mandatory Security Mechanisms

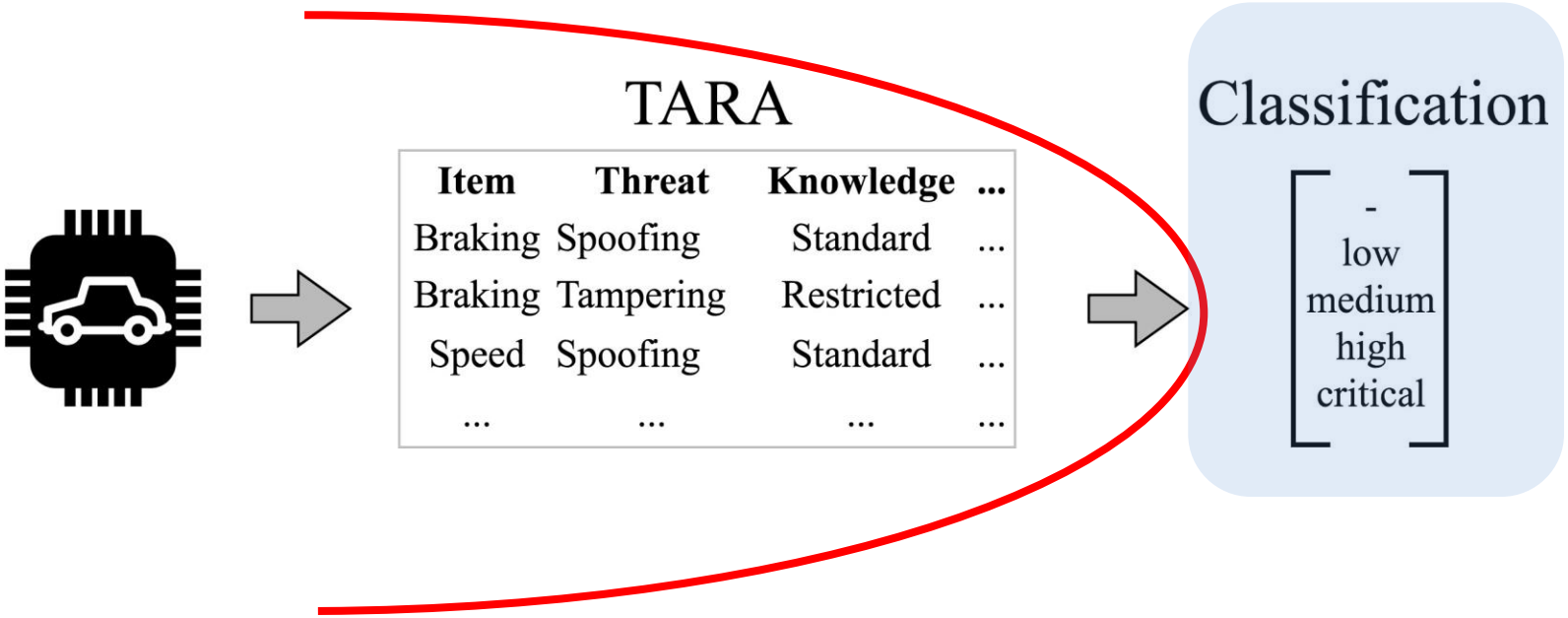
TARA

Item	Threat	Knowledge	...
Braking	Spoofing	Standard	...
Braking	Tampering	Restricted	...
Speed	Spoofing	Standard	...
...	...	...	...

Classification

[- low medium high critical]

From Security Requirements to Mandatory Security Mechanisms



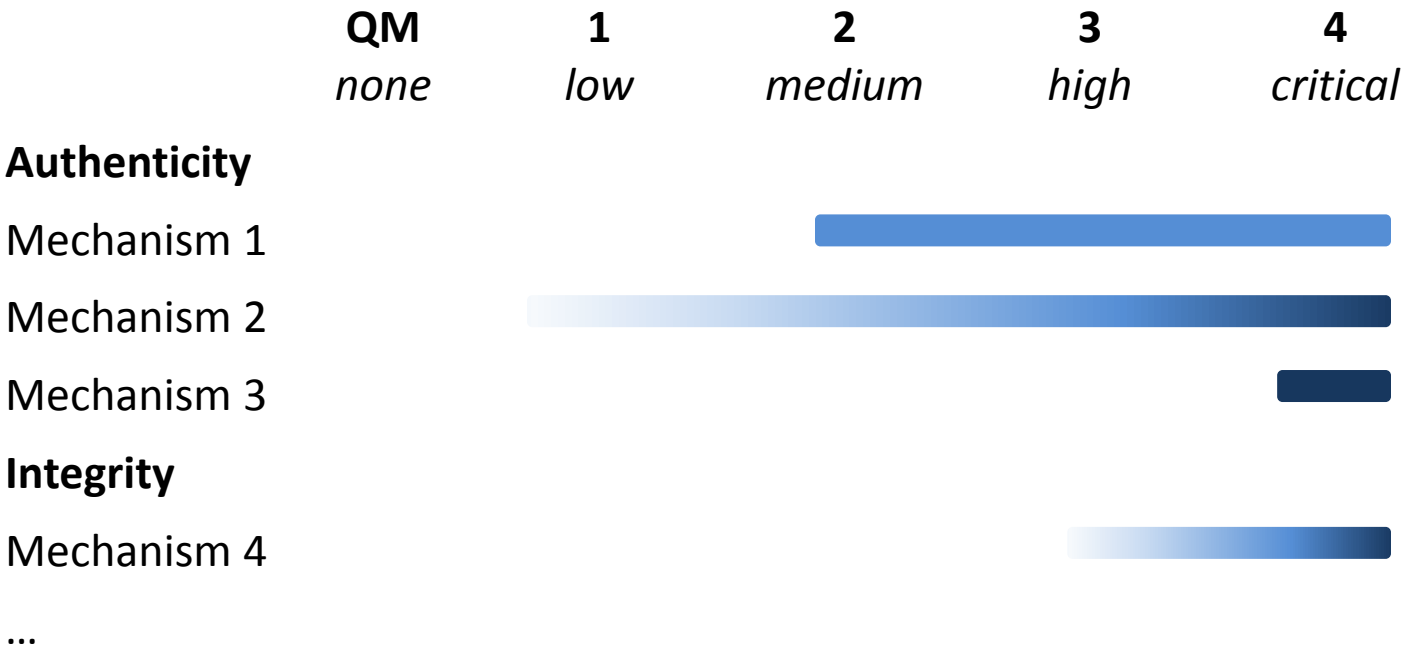
Proposed Representation of Security

- Representation as vector is necessary

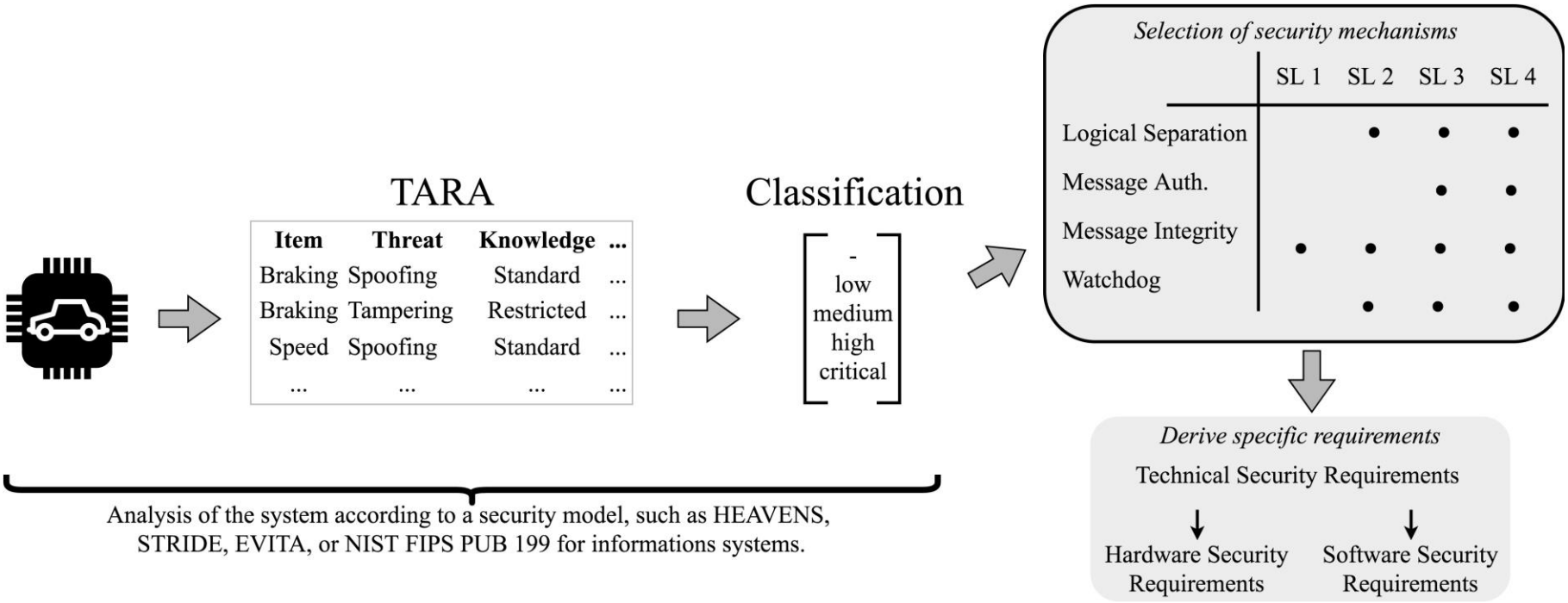
$$SL = \begin{bmatrix} Authenticity \\ Integrity \\ Non - Repudiation \\ Confidentiality \\ Availability \\ Authorisation \end{bmatrix}$$

Mapping to Security Mechanisms

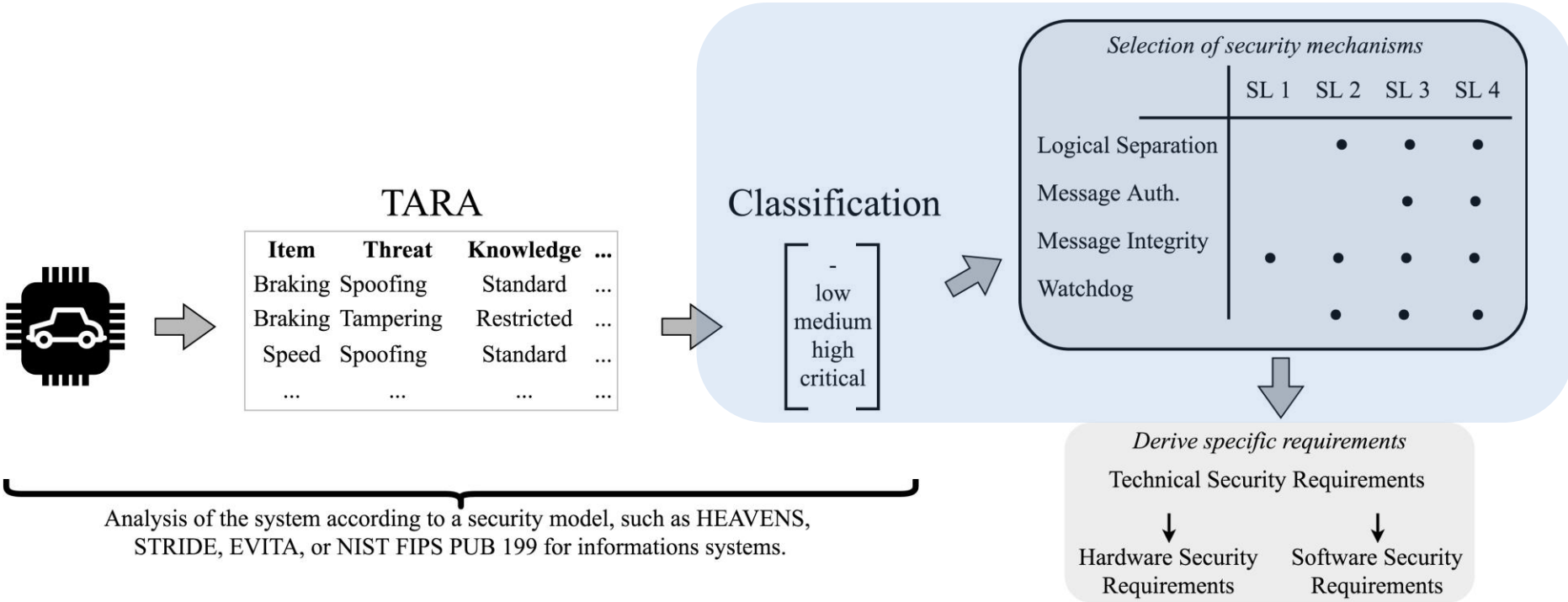
Mechanisms per security attribute depending on the level



Mapping to Security Mechanisms



Mapping to Security Mechanisms



Standards and Guidelines

- **IEC 62443/ISA 99** – Standard for industrial communication network
- **NIST FIPS PUB 199** – Standard for Security Categorization Federal Information and Information Systems
- **NIST SP 800-53** – Security and Privacy Controls for Federal Systems and Organizations
- Connected Vehicles Pilot Development – New York City
- UNECE task force on cybersecurity and over-the-air issues

Identified Mechanisms

		SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key			•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading		•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot				•	•
	IN.4 [HW] Physical protection against tampering				•	•
	IN.5 [HW] Detection of physical tampering		•	•	•	•
Authenticity	AU.1 [MSG] Message Authentication Code (MAC) with session key				•	•
	AU.2 [FW] Verify authenticity of firmware when upgrading using digital signatures[a]		1	1	2	2
	AU.3 [FW] Verify authenticity of firmware/functions on boot using digital signatures[a]				1	2
	AU.4 [HW] Verify hardware authenticity					•
Non-repudiation	NR.1 [MSG] Freshness using counter or timestamp in authenticated message				•	•
	NR.2 [MSG] Audit logging				•	•
	NR.3 [MSG] Use of digital signatures for messages (signals)					•
Confidentiality	CO.1 [MSG] Encryption of messages				•	•
	CO.2 [FW] Encryption of firmware during transmission[a]				1	2
Availability	AV.1 [MSG] Limited network access – Quality of Service				•	•
	AV.2 [FW] Watchdog timer			•	•	•
Authorization and Access Control	AC.1 [MSG] Whitelisting of messages (signals) on gateways		•	•	•	•
	AC.2 [MSG] Whitelisting of messages (signals) on nodes				•	•
	AC.3 [MSG] Access control on function level				•	•
	AC.4 [MSG] Deployment of Intrusion Detection Systems				•	•
	AC.5 [MSG, FW, HW] Logical separation[a]			1	1	2
	AC.6 [MSG, FW, HW] Domain isolation				•	•
Other requirements[b]	OR.1 Fail in known state					
	OR.2 Information Input Validation					
	OR.3 Operate with least set of privileges that are necessary					
	OR.4 Compliance to secure coding guidelines					
	OR.5 Secure Logging					

Examples: Authenticity

- Required Mechanisms for each security level [1-4]

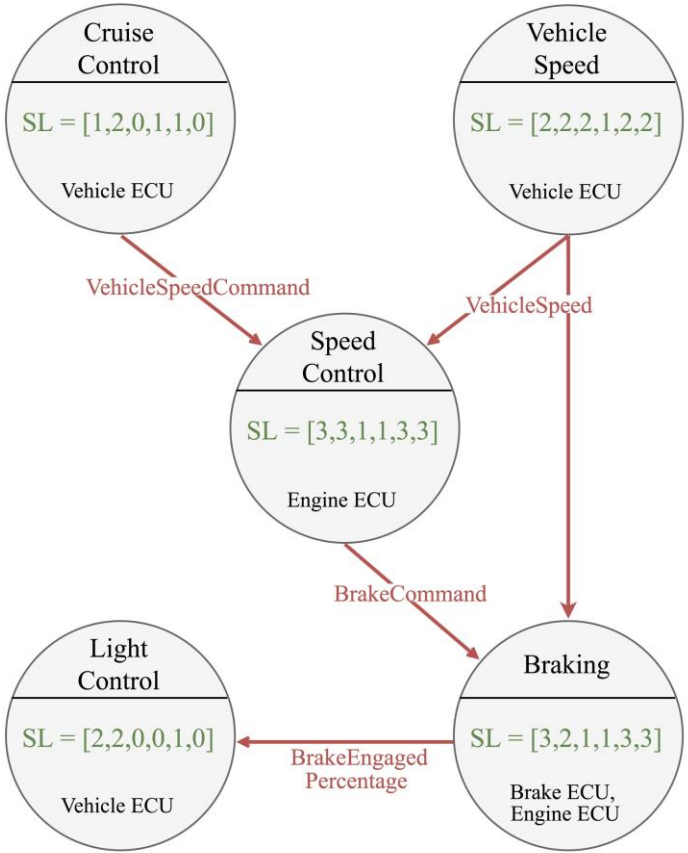
Security Level	*1*	*2*	*3*	*4*
AU.1 [MSG] Message Authentication Code (MAC) with session key			•	•
AU.2 [FW] Verify authenticity of firmware when upgrading using digital signatures[a]	1	1	2	2
AU.3 [FW] Verify authenticity of firmware/functions on boot using digital signatures[a]			1	2
AU.4 [HW] Verify hardware authenticity				•

- AU.3 “Verify authenticity of firmware/functions on boot using digital signatures”
  - Class 1: on demand verification
  - Class 2: secure boot

Examples: Authorisation

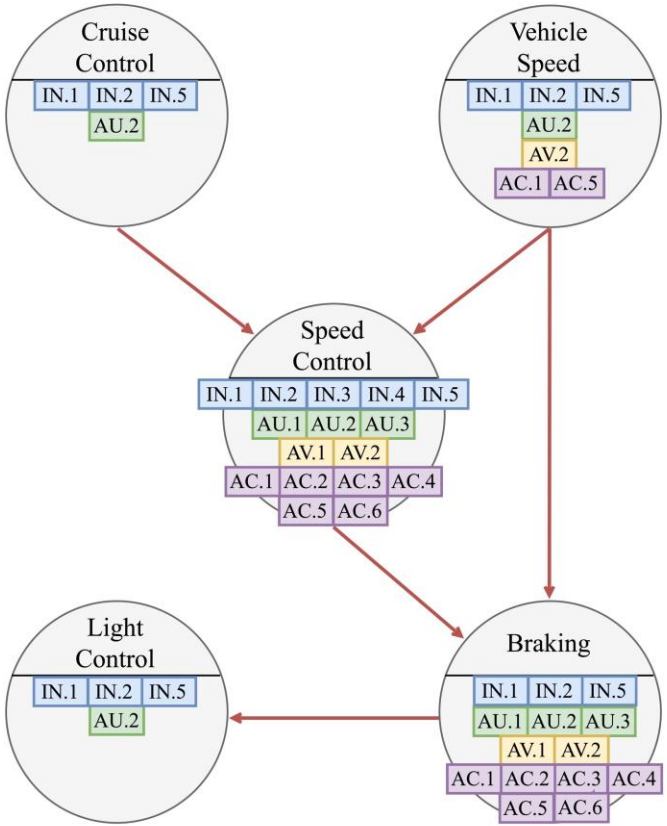
Security Level	*1*	*2*	*3*	*4*
AC.1 [MSG] Whitelisting of messages (signals) on gateways	•	•	•	•
AC.2 [MSG] Whitelisting of messages (signals) on nodes			•	•
AC.3 [MSG] Access control on function level			•	•
AC.4 [MSG] Deployment of Intrusion Detection Systems			•	•
AC.5 [MSG, FW, HW] Logical separation[a]		1	1	2
AC.6 [MSG, FW, HW] Domain isolation			•	•

Use Case: Cruise Control



Applying the Framework

- Possibility to aggregate functions and other items to ECU-level or higher
- Identified mechanisms are required to be implemented
- Exceptions only when other counter measures are implemented



IN.1 MAC with pre-shared key
IN.2 Verify firmware integrity when upgrading
IN.3 Verify firmware integrity on start
IN.4 Protection against physical tampering
IN.5 Detection of physical tampering
AU.1 MAC with session key
AU.2 Verify firmware authenticity when upgrading
AU.3 Verify firmware authenticity on start
AV.1 Limited network access, e.g., QoS
AV.2 Watchdog timer
AC.1 Whitelisting on gateways
AC.2 Whitelisting on nodes
AC.3 Access control on function level
AC.4 Intrusion Detection System
AC.5 Logical separation
AC.6 Domain isolation

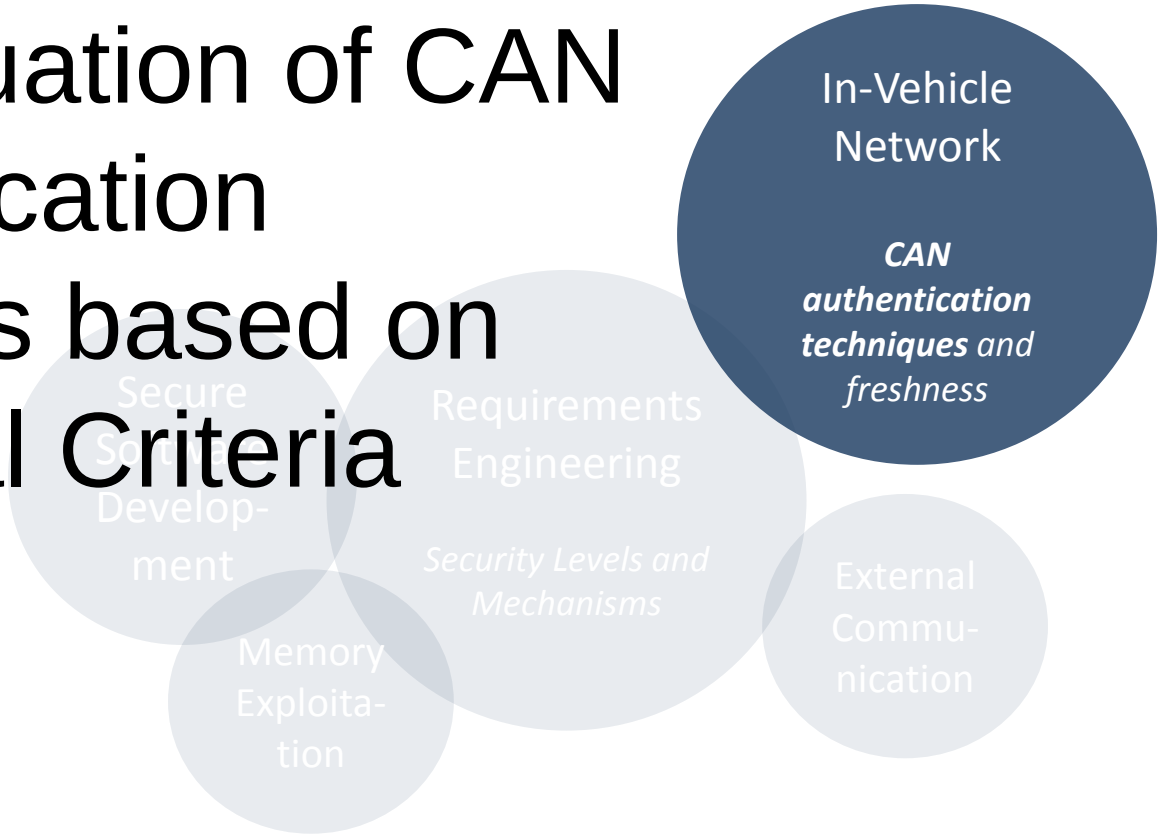
Advantages

- Strict rule-set to fulfil basic security requirements
- Better understanding of the required mechanisms between different parties
- See dependencies between safety and security in an early stage

Summary

- Representation of security as a vector
- Mapping between security levels and security mechanisms/design rules
- Provide basic security requirements
- Demonstrated with Cruise Control use case
- Verified with industrial partner

An Evaluation of CAN Authentication Solutions based on Industrial Criteria



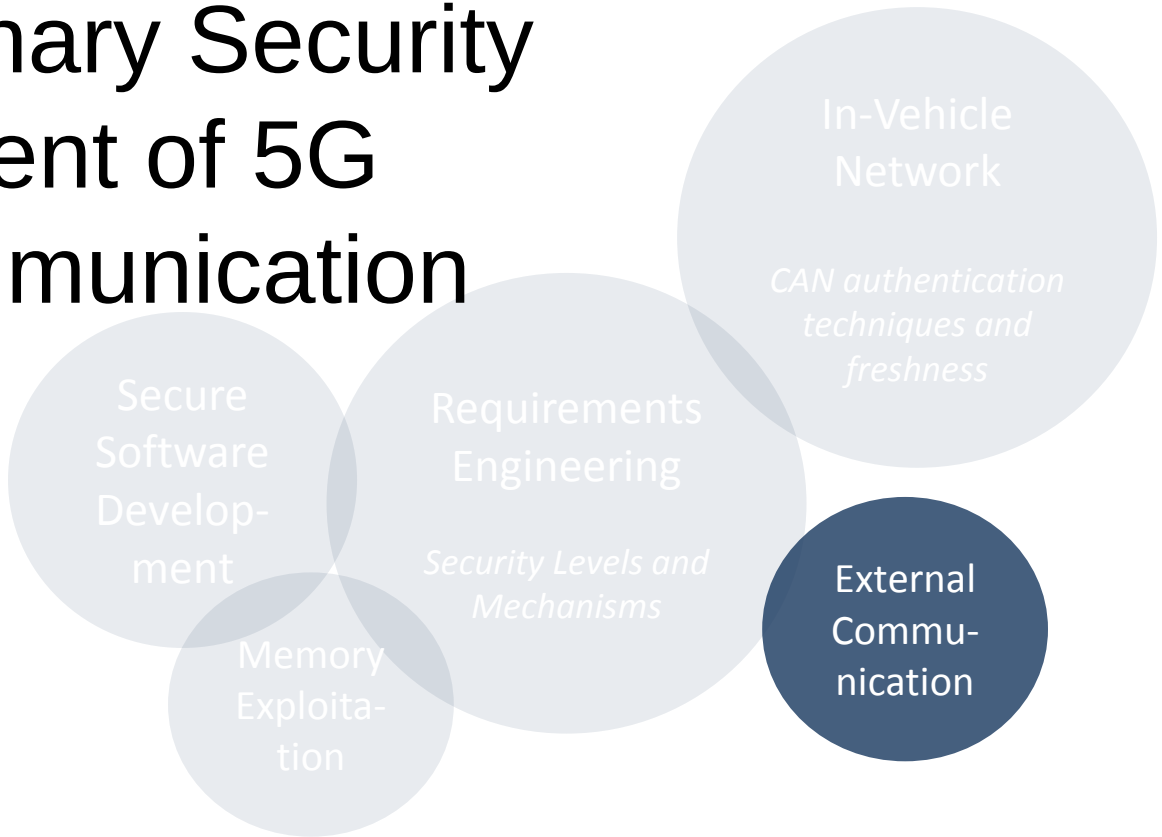
An Evaluation of CAN Authentication Solutions based on Industrial Criteria

- **IR 1** Cost Effectiveness
- **IR 2** Backward Compatibility
- **IR 3** Repair and Maintenance
- **IR 4** Implementation Details
- **IR 5** Acceptable Overhead

An Evaluation of CAN Authentication Solutions based on Industrial Criteria

Message Authentication Solution	IR 1 Cost Effectiveness	IR 2 Backward Compatibility	IR 3 Repair and Maintenance	IR 4 Implementation Details	IR 5 Acceptable Overhead	Approx. Security Level[1]
CANAuth [7]	✗	✗	✗	✗	✗	Strong
SchweppeAuth [8]	✗	✗	✓	✓	✗	Strong
LiBrA-CAN [9]	✓	✗	✓	✓	✗	Strong
LinAuth [10]	?	?	?	✗	?	Medium
MaCAN [11]	✓	✓	✓	✗	✗	Medium
CaCAN [12]	✓	✗	✓	✓	?	Weak
VeCure [13]	?	✓	?	✓	?	Medium
WooAuth [14]	✓	✗	✓	✓	✓	Medium
VatiCAN [15]	✓	✓	✓	✓	?	Medium
WeisglassAuth [16]	✓	✗	✗	✓	?	Medium

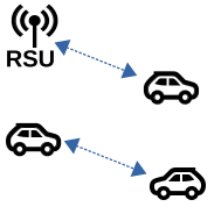
A Preliminary Security Assessment of 5G V2X Communication



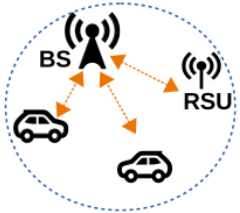
Cooperative Intelligent Transportation System

- C-ITS
  - Safety application
  - Traffic management
- C-ITS enablers
  - 802.11p (ETSI ITS-G5, IEEE WAVE)
  - Cellular V2X (C-V2X)

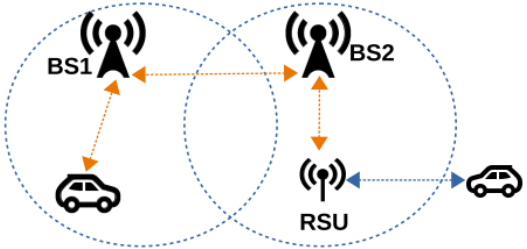
V2X Communication



(a) Direct communication
(802.11p or PC5)



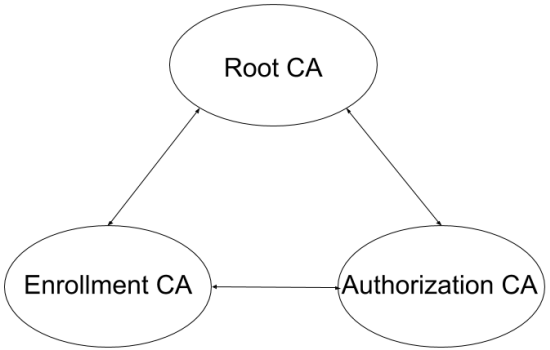
(b) Fully network-assisted
(4G/5G)

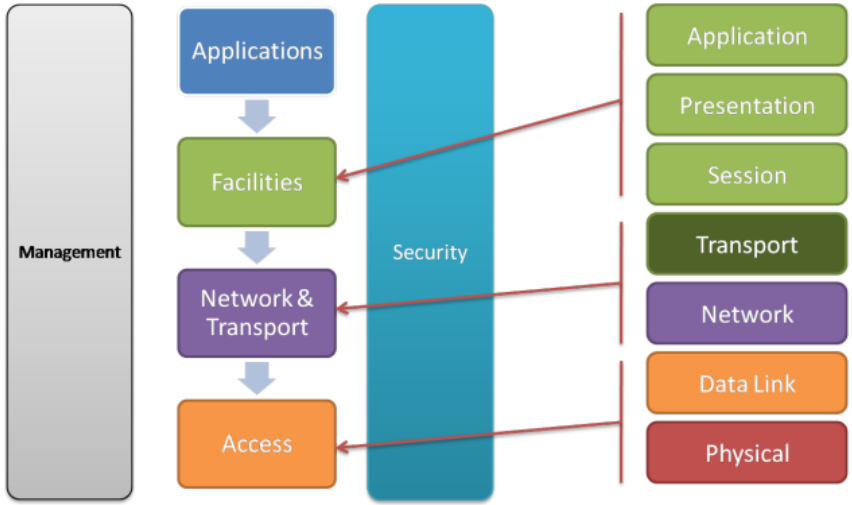


(c) Semi network-assisted
(4G/5G + 802.11p or PC5)

ETSI ITS Security Architecture

- V2X security and privacy concerns





Security Requirements of ETSI ITS Use Cases

Applications Class	Application	Use case	V2X	Conf.	Integ.	Avail.	Authen.	Priv.
Active Road Safety	Driving Assistance - Cooperative Awareness	Emergency vehicle warning	V	0	2	2	2	2
		Slow vehicle indication	V	0	2	2	2	2
		Intersection collision warning	VR	0	2	2	2	2
		Overtaking vehicle warning	V	0	2	2	2	2
		Lane change	V	0	2	2	2	2
		Glare reduction	V	0	2	2	2	2
		Motorcycle approaching indicator	VR	0	2	2	2	2
		Emergency electronic brake lights	VRN	0	2	2	2	2
		Stationary vehicle	VRN	0	2	2	2	2
	Driving Assistance - Road Hazard Warning	Wrong way driving warning	VRN	0	2	2	2	1
		Traffic condition warning	VRN	0	2	2	2	1
		Signal violation warning	R	0	2	2	2	0
		Roadwork warning	VR	0	2	2	2	0
		Collision risk warning	VR	0	2	2	2	1
		Collision unavoidable	VR	0	2	2	2	1
		Decentralized floating car data	VRN	0	2	2	2	1
Cooperative Traffic Efficiency	Speed Management	Regulatory / contextual speed limits notification	RN	0	2	1	2	0
		Traffic light optimal speed advisory	R	0	2	1	2	0
	Cooperative Navigation	Traffic information and recommended itinerary	R	0	2	1	2	0
		Enhanced route guidance and navigation	RN	0	2	1	2	0
		Limited access warning and detour notification	R	0	2	1	2	0
		In-vehicle signage	R	0	2	1	2	0
		Point of Interest notification	R	0	2	1	2	0
Cooperative Local Services	Location Based Services	Automatic access control and parking management	RN	2	2	1	2	2
		Local electronic commerce	RN	2	2	1	2	2
		Media downloading	RN	2	2	1	2	2
		Insurance/financial services	RN	2	2	1	2	2
Global Internet Services	Communities Services	Fleet management	RN	2	2	1	2	2
		Loading zone management	RN	2	2	1	2	2
	ITS Station Life Cycle Management	Vehicle software/data provisioning and update	RN	2	2	2	2	2
		Vehicle-RSU sensor data calibration	RN	0	2	1	2	0

5G V2X

- 5G New Radio
- 5GAA: 5G for V2X
  - Latency
  - Throughput
  - Reliability
- Millimetre waves
- Beamforming
- Massive MIMO
- Physical layer security

Physical Layer Security

- Millimetre waves and beamforming
- Massive MIMO
- C-V2X Security for ETSI ITS use cases
  - Direct Communication
    - No security advantages
  - Semi-Assisted Network
    - No security advantages except for the fully network assisted part
  - Fully network assisted
    - Active Road Safety
    - Cooperative Traffic Efficiency
    - Cooperative Local Services and Global Internet Services

Applications Class	Application	Use case	V2X	Conf.	Integ.	Avail.	Authen.	Priv.
Active Road Safety	Driving Assistance - Cooperative Awareness	Emergency vehicle warning	V	0	2	2	2	2
		Slow vehicle indication	V	0	2	2	2	2
		Intersection collision warning	VR	0	2	2	2	2
		Overtaking vehicle warning	V	0	2	2	2	2
		Lane change	V	0	2	2	2	2
		Glare reduction	V	0	2	2	2	2
	Driving Assistance - Road Hazard Warning	Motorcycle approaching indicator	VR	0	2	2	2	2
		Emergency electronic brake lights	VRN	0	2	2	2	2
		Stationary vehicle	VRN	0	2	2	2	2
		Wrong way driving warning	VRN	0	2	2	2	1
		Traffic condition warning	VRN	0	2	2	2	1
		Signal violation warning	R	0	2	2	2	0
		Roadwork warning	VR	0	2	2	2	0
		Collision risk warning	VR	0	2	2	2	1
		Collision unavoidable	VR	0	2	2	2	1
		Decentralized floating car data	VRN	0	2	2	2	1
Cooperative Traffic Efficiency	Speed Management	Regulatory / contextual speed limits notification	RN	0	2	1	2	0
		Traffic light optimal speed advisory	R	0	2	1	2	0
	Cooperative Navigation	Traffic information and recommended itinerary	R	0	2	1	2	0
		Enhanced route guidance and navigation	RN	0	2	1	2	0
		Limited access warning and detour notification	R	0	2	1	2	0
		In-vehicle signage	R	0	2	1	2	0
		Point of Interest notification	R	0	2	1	2	0
Cooperative Local Services	Location Based Services	Automatic access control and parking management	RN	2	2	1	2	2
		Local electronic commerce	RN	2	2	1	2	2
		Media downloading	RN	2	2	1	2	2
Global Internet Services	Communities Services	Insurance/financial services	RN	2	2	1	2	2
		Fleet management	RN	2	2	1	2	2
		Loading zone management	RN	2	2	1	2	2
	ITS Station Life Cycle Management	Vehicle software/data provisioning and update	RN	2	2	2	2	2
		Vehicle-RSU sensor data calibration	RN	0	2	1	2	0

HoliSec

Holistic Approach to Improve Data Security

Thank you for your attention!

Publications

- N. Nowdehi, A. Lautenbach, and T. Olovsson, “In-vehicle can message authentication: An evaluation based on industrial criteria”, in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Sep. 2017, pp. 1–7. DOI: 10.1109/VTCFall.2017.8288327.

- A. Lautenbach, M. Almgren, and T. Olovsson, “What the stack? on memory exploitation and protection in resource constrained automotive systems”, in Critical Information Infrastructures Security, G. D’Agostino and A. Scala, Eds., Cham: Springer International Publishing, 2018, pp. 185–193, ISBN: 978-3-319-99843-5

- T. Rosenstatter and T. Olovsson, “Open problems when mapping automotive security levels to system requirements”, in *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems - Volume 1: VEHITS,* INSTICC, SciTePress, 2018, pp. 251–260, ISBN: 978-989-758-293-6. DOI: 10.5220/0006665302510260.

- T. Rosenstatter and T. Olovsson, “Towards a standardized mapping from automotive security levels to security mechanisms”, in *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, Nov. 2018, pp. 1501–1507. DOI: 10.1109/ ITSC.2018.8569679.

Publications

- A. Lautenbach, M. Almgren and T. Olovsson, “Understanding Common Automotive Security Issues and Their Implications” presented at International Workshop on Interplay of Security, Safety and System/Software Architecture 2018

- A. Lautenbach, N. Nowdehi, T. Olovsson and R. Zaragatzky, ”A Preliminary Security Assessment of 5G V2X”, will be presented at VTC-Spring 2019.

- T. Rosenstatter, C. Sandberg and T. Olovsson, “Improving AUTOSAR’s Counter-based Solution for Freshness of Authenticated Messages in Vehicles” under submission.