HoliSec

Holistic Approach to Improve Data Security

State of the Art of Secure Vehicular Communication and Design

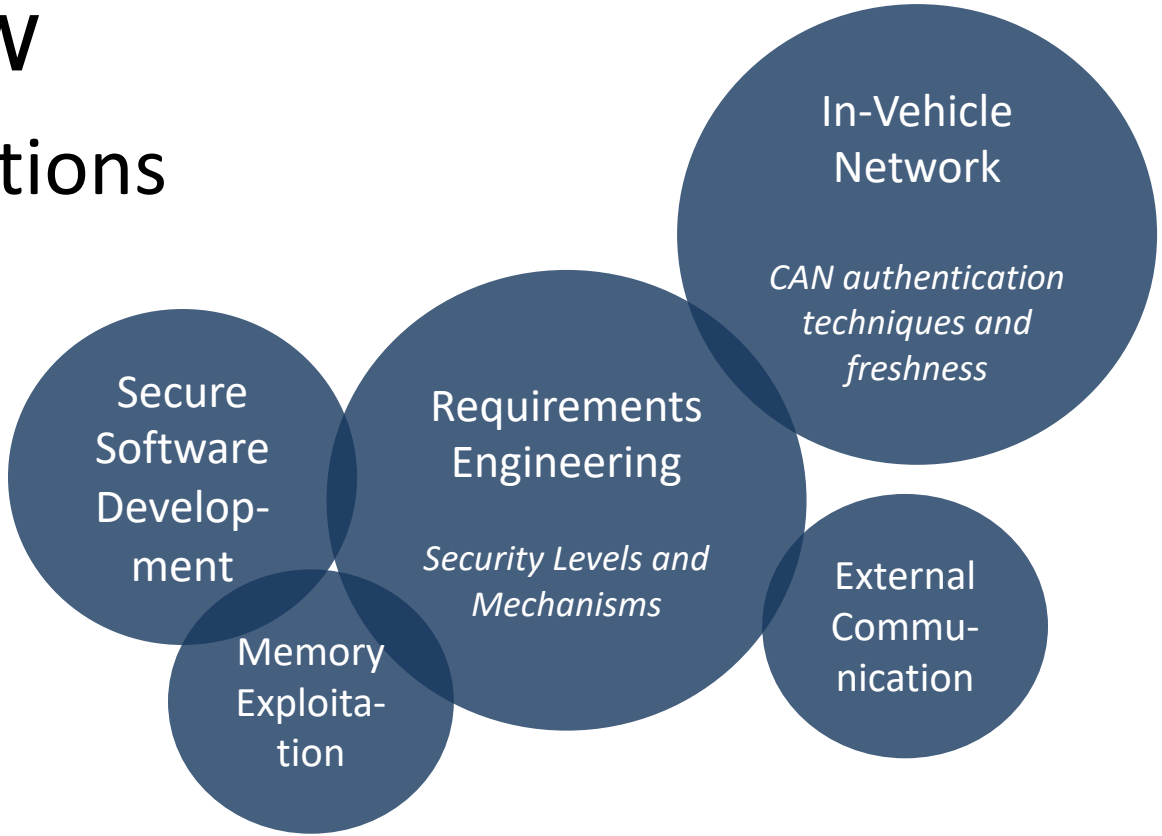
A. Lautenbach, N. Nowdehi, **T. Rosenstatter**

October 10, 2019. Time 09:35 – 09:55

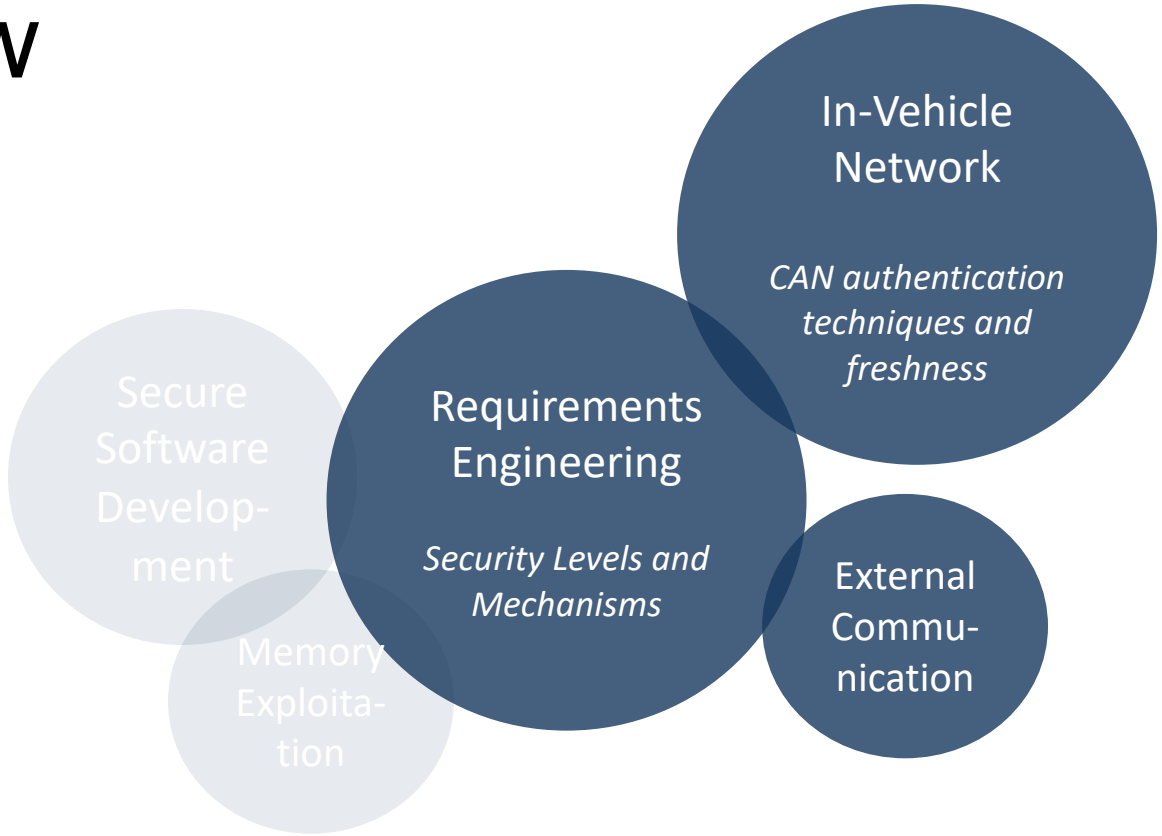
VINNOVA FFI VOLVO VOLVO ARC CORE CHALMERS ASSURED SECURITY CONSULTANTS RI. SE Research Institutes of Sweden

Overview

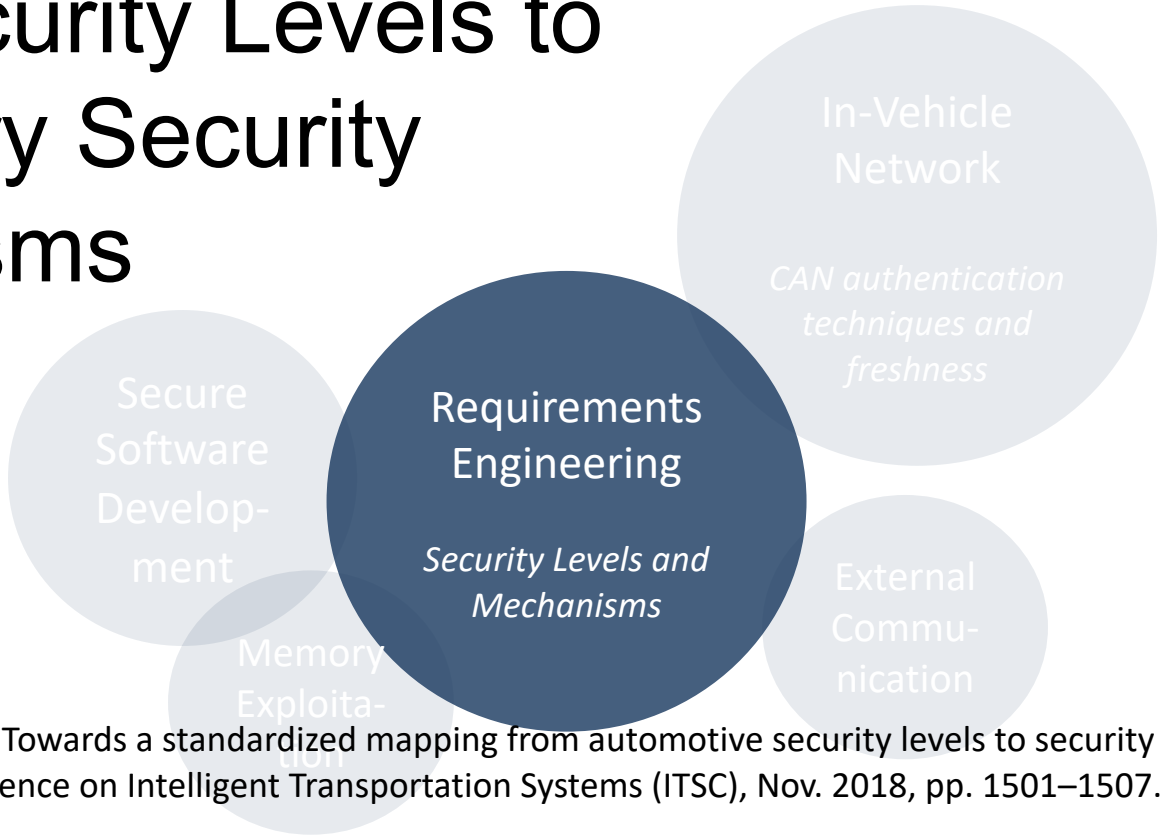
- 8 publications



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 Levels to Mandatory Security Mechanisms



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.

From Security Levels to Mandatory Security Mechanisms

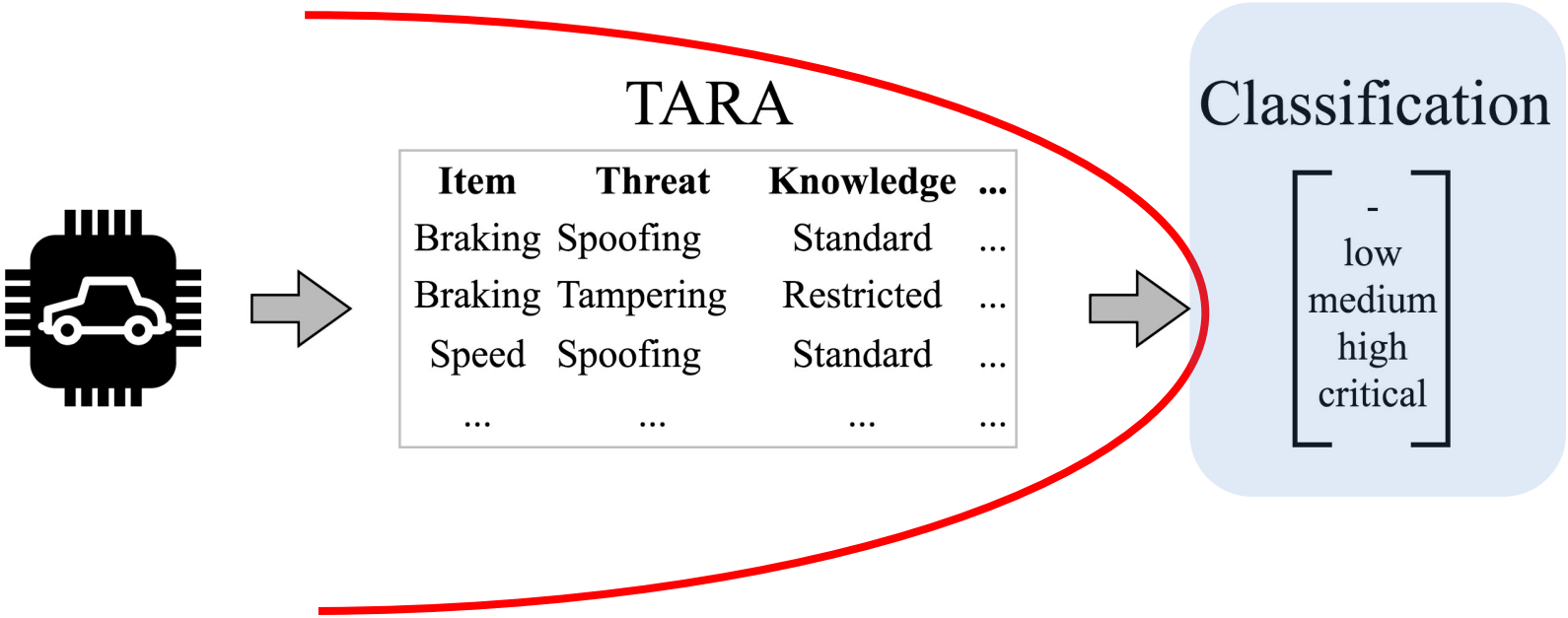
TARA

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

Classification

[- low medium high critical]

From Security Requirements to Mandatory Security Mechanisms



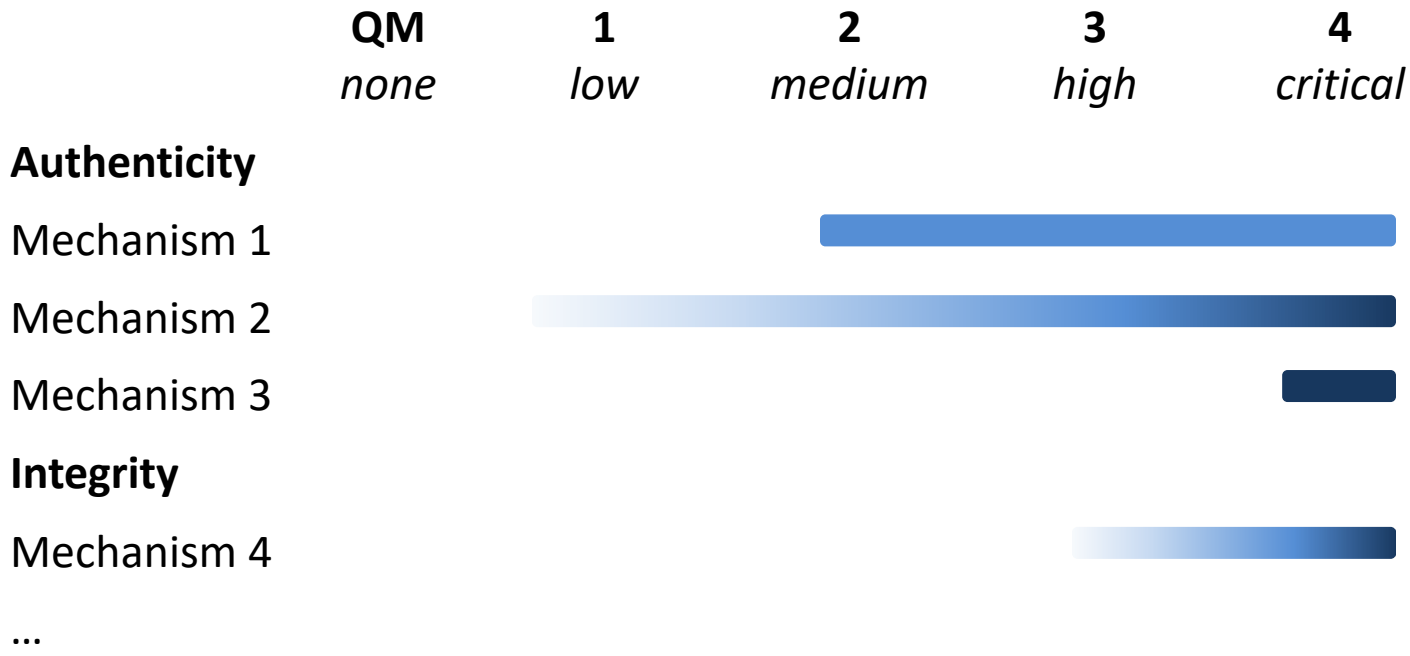
Proposed Representation of Security

- Representation as vector is necessary

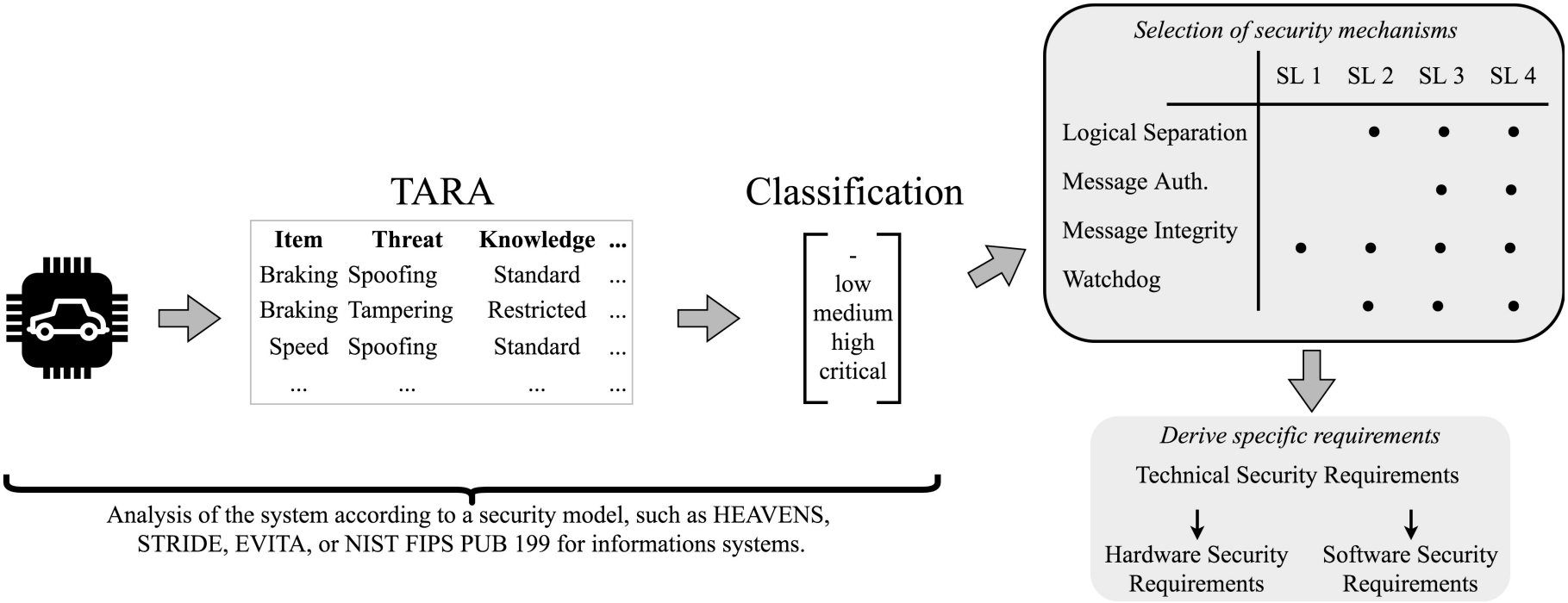
$$SL = \begin{bmatrix} Authenticity \\ Integrity \\ Non - Repudiation \\ Confidentiality \\ Availability \\ Authorisation \end{bmatrix}$$

Mapping to Security Mechanisms

Mechanisms per security attribute depending on the level



Mapping to Security Mechanisms



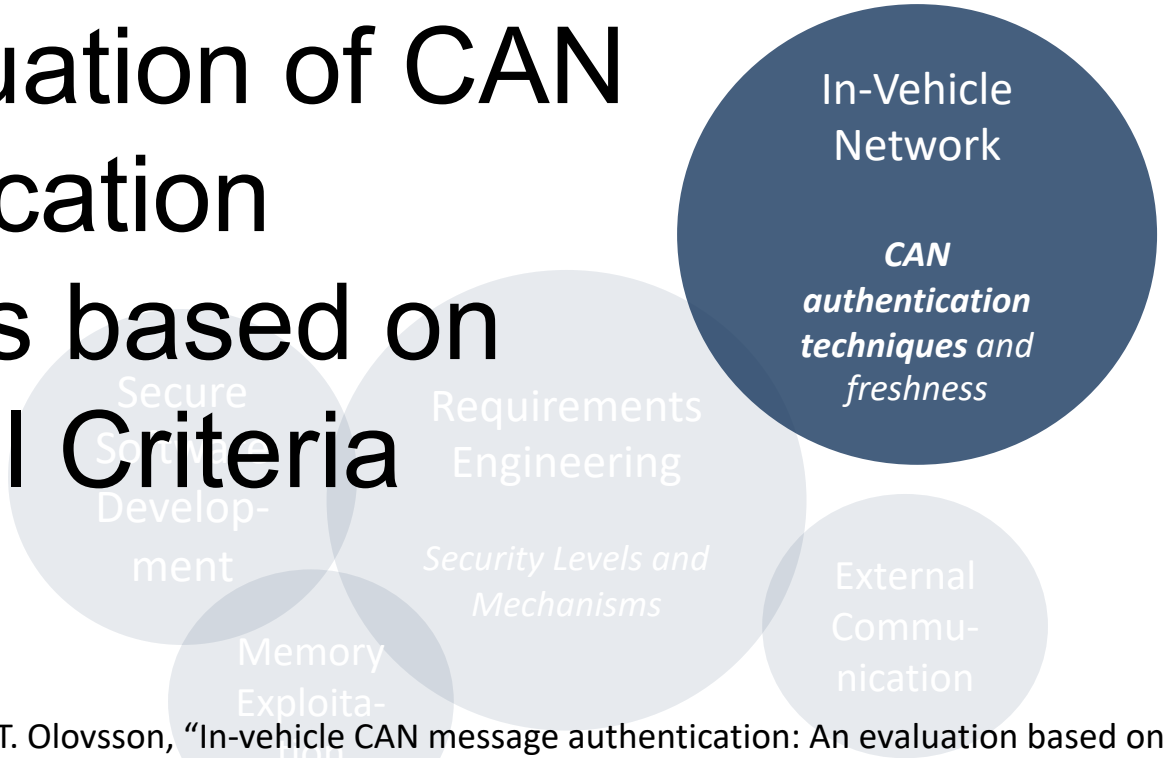
Identified Mechanisms

		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					

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

An Evaluation of CAN Authentication Solutions based on Industrial Criteria



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.

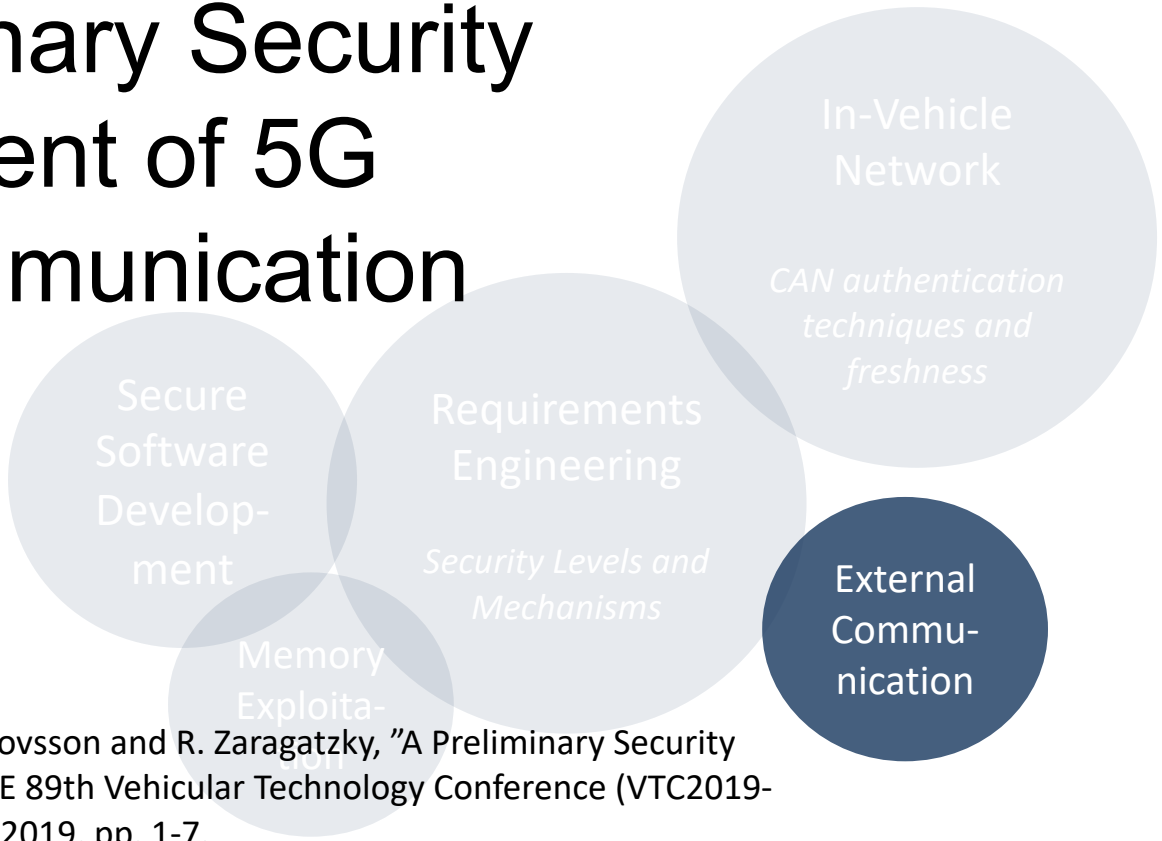
An Evaluation of CAN Authentication Solutions based on Industrial Criteria

- **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



A. Lautenbach, N. Nowdehi, T. Olovsson and R. Zaragatzky, ”A Preliminary Security Assessment of 5G V2X”, 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-7.

Research Question

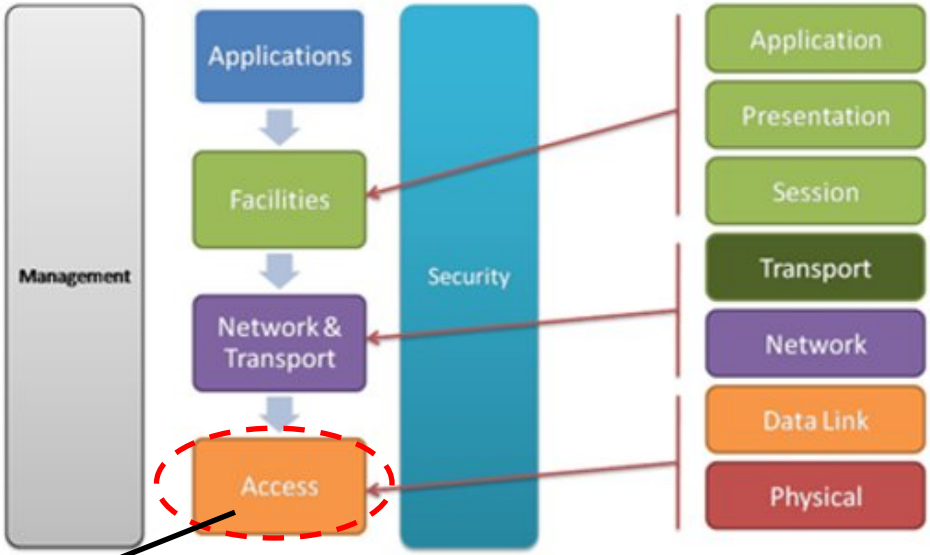
Can the 5G NR features change the way the existing V2X standards handle security?

- V2X application security requirements
- How the existing V2X standards handle these requirements?
- 5G NR features and how they can improve security

Cooperative Intelligent Transportation System

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

ETSI ITS Security Architecture

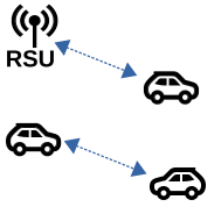


Not covered by the security layer!

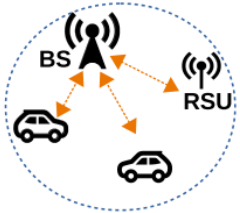
5G V2X

- Provides lower latency and higher throughput
- Physical layer security
  - As long as the environment is sufficiently stable, a wireless channel has a unique fingerprint of physical properties that identifies it, which can be used to authenticate a previously established connection
- Millimeter waves (6 GHz)
- Massive MIMO (100 ports)
- Beamforming (Focused stream of data to specific user)
- Millimeter waves + Massive MIMO + Beamforming = highly directional communication that can be used to authenticate based on sender/receiver location

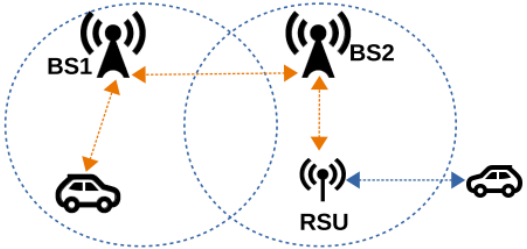
V2X Communication



(a) Direct communication
(802.11p or PC5)

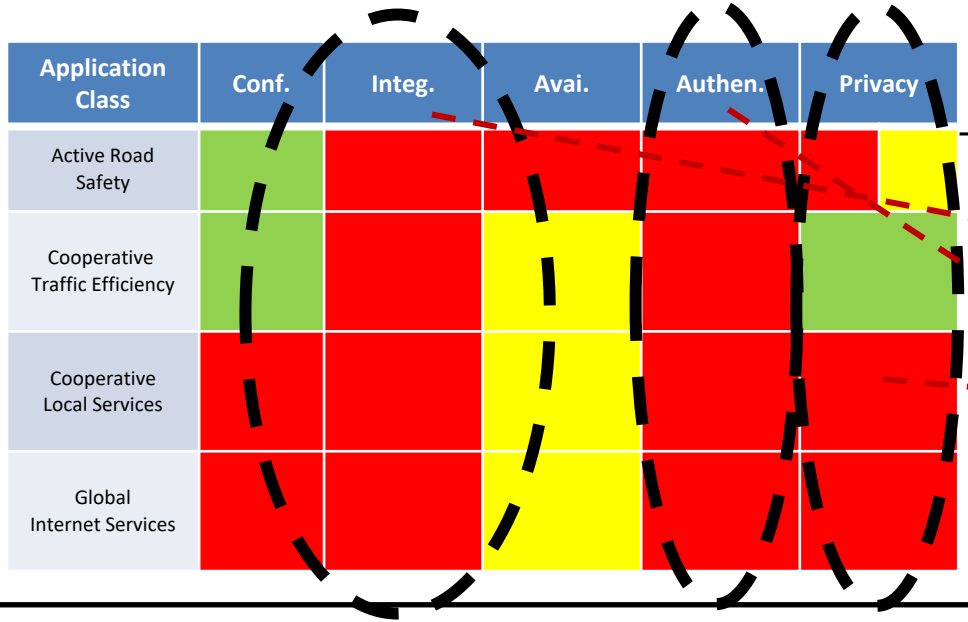


(b) Fully network-assisted
(4G/5G)



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

CAN 5G NR Improve C-ITS Security



- 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
    - Implicitly covered by the cellular network (all messages are signed and encrypted)
    - Re-authentication via the physical security
    - Partly covered (encryption), but improved by highly directional communication
      - ID revealed during authentication
      - ID pseudonymization is required

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”, 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-7.

- T. Rosenstatter, C. Sandberg and T. Olovsson, “Extending AUTOSAR’s Counter-based Solution for Freshness of Authenticated Messages in Vehicles” accepted at 24th IEEE Pacific Rim International Symposion on Dependable Computing (PRDC 2019).