Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles

Christian Plappert, Andreas Fuchs

Wednesday 6th December, 2023

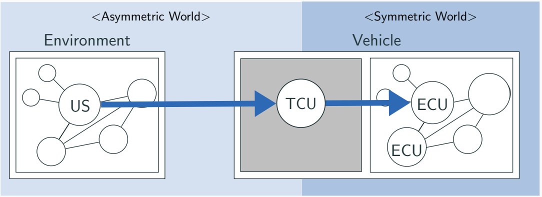
Fraunhofer SIT | ATHENE

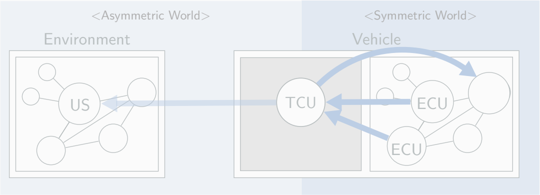
This presentation is based on Christian Plappert and Andreas Fuchs. "Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles". In: *Proceedings of the 39th Annual Computer Security Applications Conference*. ACSAC '23. Austin, TX, USA: Association for Computing Machinery, 2023. ISBN: 9798400708862. DOI: 10.1145/3627106.3627135. URL: https://doi.org/10.1145/3627106.3627135

Artifacts are evaluated and available at https://github.com/cplappert/update-distribution

Secure OTA Updates for Connected Vehicles

- Part 1: Secure Update Distribution (now)
- Part 2: Secure Update Installation Reporting (follow-up)





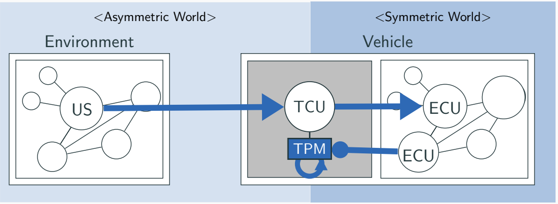
Introduction

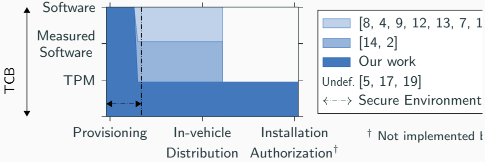
- Connected Vehicle is more and more exposed to the environment
  - More interfaces to the outside world
  - More complex vehicle software
- Cyberattacks
  - Monetary and safety implications
- OTA Updates as solid mitigation strategy
  - Prevents costly recalls
- Securing OTA Updates are challenging task
  - Full controller/network access required

wired.com [3]

Contribution

- Secure OTA update distribution and installation coordination system
- Address requirements from standards and regulations
  - Automotive Domain, UNECE R155/156, ISO 21434, Uptane
- TPM as central trust anchor in the vehicle
  - Cryptographic Proxy
  - Update Installation Coordination
- Benefits
  - Security Policies directly enforced in TPM
  - Solution does not rely on (Measured) Software
  - All symmetric keys stored on TPM, Backend only needs signature keys

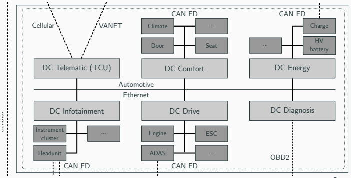




Background: Automotive Domain

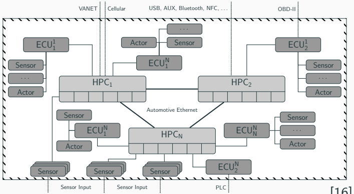
- Heterogeneous networks
- Different topologies
- Various interfaces
- Past: Security limited
  - Symmetric, MACs (SecOC)
- Legacy/resource-constraint components remain

Currently:
Domain-based Architectures



[20]

Upcoming:
Centralized/Zone Architectures



[16]

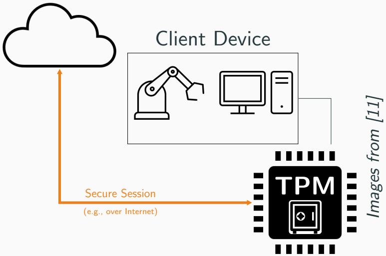
Future:
?

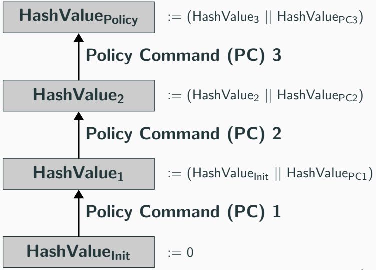
?

Background: TPM

- Security Coprocessor standardized by Trusted Computing Group (TCG)
- Provides tamper-proof shielded location
  - Generation/storage of cryptographic keys and storage of arbitrary data (e.g., integrity measurements, counters)
  - Execution of (cryptographic) operations
  - NV memory (arbitrary, counter, bit field, etc.)
- Remote authorization concepts
  - Session-based key/data authorization (audit)
  - Enhanced Authorization
    - Concatenate usage constraints to a “TPM policy”
    - Policy needs to be successfully processed by TPM to authorize key/data usage
    - TPM supports different constraining policy commands

      Time, usage, software state, command, ...



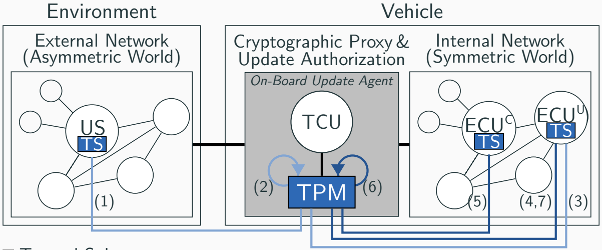


Background: Standards/Regulations

- UNECE Regulations 155 & 156
  - United Nations Economic Commission for Europe (UNECE) for Harmonization of Vehicle Regulations
  - Adoption of the first international regulations governing vehicle cybersecurity
  - Europe, Japan, Republic of Korea → third of global production
  - Mandatory for new vehicle types from July 2022, all vehicles from July 2024
  - UNECE R 155: Cyber security and cyber security management system
  - UNECE R 156: Requirements for Software update and software updates management system
- ISO 21434: "Road vehicles – Cybersecurity engineering"
  - Cybersecurity engineering in concept phase of automotive engineering
  - Execution of a comprehensive Threat Analysis and Risk Assessment (TARA)
- Related work
  - Uptane (→ ISO 24089: "Road vehicles – Software update engineering")
    - Best practices

System Design – System Model and High-Level Concept

- Abstract automotive reference architecture
  - Environment, TCU, internal network (ECU^U, ECU^C)
- TPM is primary security provider of the system
  - Security of ECUs may remain lightweight
- 2 Security Building Blocks (SBBs)
  1. SBB1: Authenticated Update Distribution
  2. SBB2: Coordinated Update Authorization



Trusted Subsystem:
US: Air gap, TCU: TPM, $ECU^{U/C}$: HSM/DICE/TZ/...
SBB1: Secure Update Distribution:
(1) Asymmetric Channel, (2) Rekeying, (3) Symmetric Channel
SBB2: Secure Update Authorization:
(4) Update Installation Request, (5) Request Vehicle State Condition, (6) Conditional Authorization, (7) Update Installation Authorization

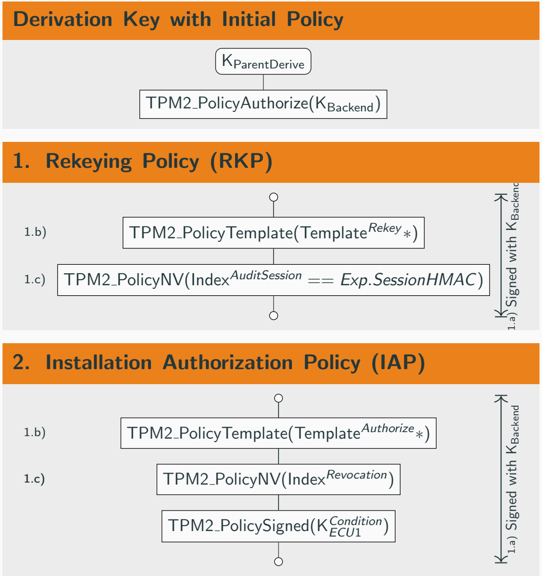
System Requirements

Requirements

- R01 & R02: Secure host processes & communication
- R03: Secure Key Management
- R04: Conditional Update
    - Constraints to the update process (enough remaining battery power, driver approval, immobilizer activated)
- R05: Unauthorized Rollback Prevention
- R06: Offline Signing Keys
- R07: Correct Updates
- R08: Semi-Offline Capabilities
- R09: Off-ECU Security Enforcement
- R10: Feasibility

System Specification – Policy Design

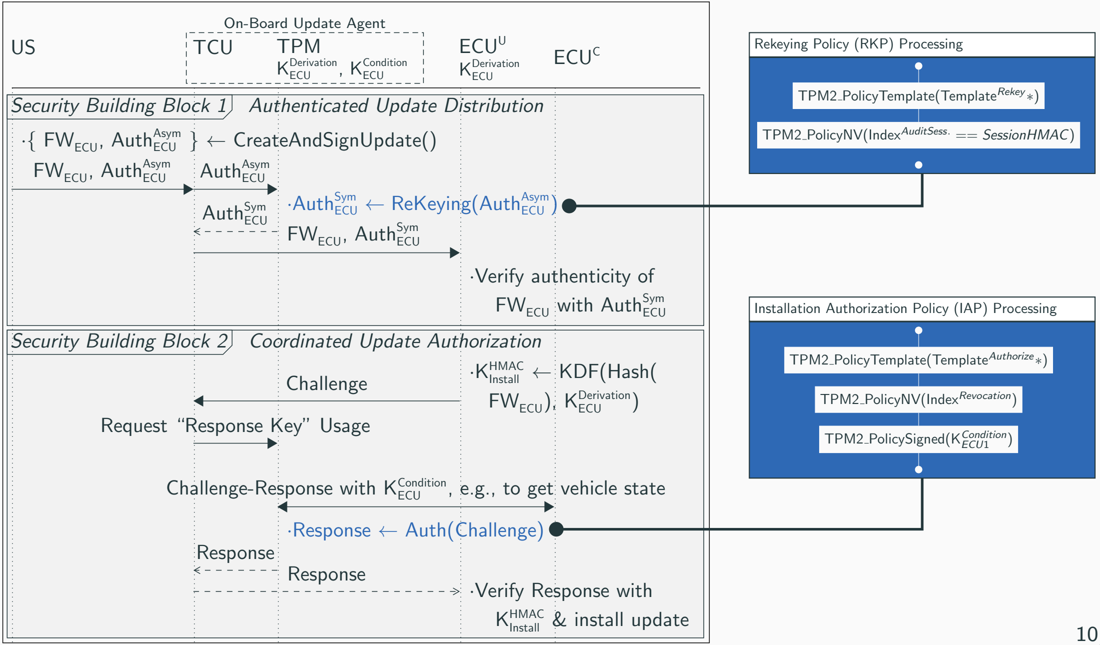
- Goals
  - a) Only backend may authorize key derivation
  1. Rekeying
     - b) Derive update unique keys
     - c) Derive only if signature is valid
  2. Update Authorization
     - b) Derive installation unique keys
     - c) Enable revocation
     - d) Enforce restrictions from standards/regulations



† $K_{ParentDerive}$ securely contains DerivationSecret

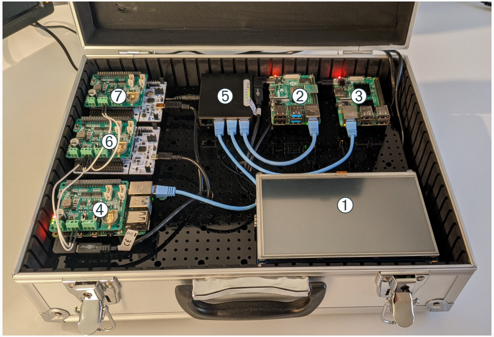
* $Template^{Rekey} := (Hash(FW_{ECU}))$

System Specification – High-Level Update Protocol



Evaluation – Prototypical Implementation

- Raspberry Pi + TPM RPi Integration Board
  - Update Target and Condition ECUs
- TPM2 Software Stack / Tools
  - Policies: FAPI
  - Rekeying: ESAPI implementation extension (Key Derivation)
- Cryptographic Primitives & Schemes
  - Asymmetric World: RSA/ECC-based schemes (signature for update bundles and policies)
  - Symmetric World: HMAC (MAC for update bundles and key derivation)



① Backend ② Update Agent (with TPM) ③ ECU^U ④ ECU^C
⑤ Ethernet Switch ⑥/⑦ CAN (FD) Subnetwork

- Artifacts are evaluated and available at https://github.com/cplappert/update-distribution

Evaluation – Automotive Feasibility Evaluation (1)

1. Address security requirements
   - Attacker model, reference architecture, automotive standards and regulations, related work
2. TPM as “crypto-proxy”
   - Addresses heterogeneous environment
   - Translates asymmetric backend world to symmetric in-vehicle world
   - Symmetric keys in shielded location of TPM
3. TPM as primary vehicle trust anchor
   - Installation authorization coordinator
   - Security overhead on resource-constraint ECUs is minimized
4. Design enables reasonably low overheads for both transmission size and on computational level

Evaluation – Automotive Feasibility Evaluation (2)

- Network & storage requirements
  - Policies and asymmetric schemes in backend world
    - 1.6 kB – 4.1 kB
  - Challenge-Response in the vehicle
    - 32 B (SBB1) – 256 B (SBB2)

	SBB	Data (Size [Byte])	Total Size [Byte]
External	SBB1†	$\text{Auth}_{\text{ECU}}^{\text{Asym}}$ (71/256), Enc^{Salt} (68/256), N_{TPM} (32), N_{T} (32), RKP (1415/1873)	1618/2449
	SBB2†	IAP with 1xECU$^{\text{C}}$	2215/2727
		IAP with 2xECU$^{\text{C}}$	2903/3415
		IAP with 3xECU$^{\text{C}}$	3591/4103
Internal	SBB1	$\text{Auth}_{\text{ECU}}^{\text{Sym}}$ (32)	32
	SBB2	C_{U} (32), R_{U}(32)	64
	SBB2	3*(C_{C} (32) + R_{C}(32)) (3*ECU$^{\text{C}}$)	192

†: The slash separates the ECC and RSA variants for asymmetric schemes.

Evaluation – Automotive Feasibility Evaluation (2)

- Network & storage requirements
  - Policies and asymmetric schemes in backend world
    - 1.6 kB – 4.1 kB
  - Challenge-Response in the vehicle
    - 32 B (SBB1) – 256 B (SBB2)
- Execution times
  - SBB1: 890 ms – 735 ms
  - SBB2: 1157 ms – 860 ms
  - → Asymmetric: Verify update and policy

Level	Operation	RSA [ms]		ECC [ms]	
1.3.	ECU^{U}	142.503	(± 7.369)	143.465	(± 6.223)
1.2.	$Network_{ECU^{U}}$	145.602	(± 1.054)	158.147	(± 0.907)
1.1.5.	HMAC	13.114	(± 0.330)	13.602	(± 0.463)
1.1.4.	Key Derivation	50.369	(± 0.745)	50.439	(± 0.768)
1.1.3.	Authorize Policy	40.940	(± 0.942)	136.922	(± 1.148)
1.1.2.2.	TPM2_PolicyNV	7.546	(± 0.522)	7.673	(± 0.546)
1.1.2.1.	TPM2_PolicyTemplate	4.587	(± 0.284)	4.691	(± 0.349)
1.1.2.	RKP Processing	21.174	(± 1.453)	21.515	(± 23.380)
1.1.1.	Verify Update	20.150	(± 0.563)	117.178	(± 0.680)
1.1.	TCU	602.255	(± 5.546)	434.054	(± 12.290)
1.	SBB1	890.359	(± 17.553)	735.666	(± 28.107)
2.5.	ECU^{C}	151.225	(± 22.566)	151.423	(± 23.577)
2.4.	$Network_{ECU^{C}}$	176.904	(± 0.847)	155.577	(± 0.950)
2.3.	ECU^{U}	132.652	(± 8.459)	132.804	(± 19.292)
2.2.	$Network_{ECU^{U}}$	80.011	(± 1.105)	74.298	(± 1.004)
2.1.6.	HMAC	13.034	(± 0.765)	12.570	(± 0.796)
2.1.5.	Key Derivation	50.399	(± 0.384)	50.625	(± 0.420)
2.1.4.	Authorize Policy	38.632	(± 2.026)	134.170	(± 1.900)
2.1.3.3.	TPM2_PolicySigned†	14.469	(± 0.654)	14.479	(± 0.649)
2.1.3.2.	TPM2_PolicyNV	7.042	(± 0.467)	6.974	(± 0.372)
2.1.3.1.	TPM2_PolicyTemplate	3.957	(± 0.384)	3.993	(± 0.479)
2.1.3.	IAP Processing	25.672	(± 1.331)	25.650	(± 1.331)
2.1.2.	ReadHMAC†	0.066	(± 0.010)	0.062	(± 0.012)
2.1.1.	GetNonce†	0.006	(± 0.002)	0.005	(± 0.002)
2.1.	TCU	616.785	(± 31.523)	346.116	(± 32.934)
2.	SBB2 (1x ECU^{C})	1157.578	(± 63.705)	860.218	(± 55.045)
2.a)	SBB2 (2x ECU^{C})	1171.004	(± 42.520)	878.562	(± 45.953)
2.b)	SBB2 (3x ECU^{C})	1187.213	(± 67.153)	992.106	(± 51.254)

†: Operation influences computational overhead for increasing ECU^{C}.

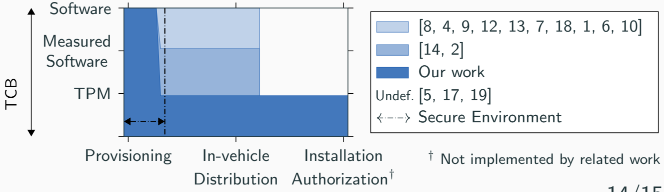
Evaluation – Comparison to Related Work

- Various OTA update types
- Link to our attacker model / functionality
  - A1: Network attacker, A2: Hijacking attacker, A3: Runtime attacker
- Comparing TCB during OTA lifecycle
- Results
  - All works not utilizing HTA focus on communication channels
    - No security against A2, A3
  - Works utilizing TPM rely on measured boot
    - No security against A3
- Only 2 works utilize rekeying, none installation authorization

Work	Type	TCB	Protection A1 A2 A3	Conditional Rekeying	Installation Authorization
[8, 4, 9]	Symmetric	SW	● ○ ○	-	○
[12, 13]	Hash	SW	● ○ ○	-	○
[7]/[18]	Hybrid	SW	● ○ ○	○ / ●	○
[19]	Blockchain	HTA?	● ? ?	○	○
[1]	Blockchain	SW	● ○ ○	○	○
[10]	Steganogr.	SW	● ○ ○	○	○
[6]	Framework	SW	● ○ ○	?	○
[5]	HSM	?	● ? ○	○	○
[17]	TPM	?	● ? ?	○	○
[14]/[2]	TPM	M-SW	● ● ○	● / ○	○
Our work	TPM	TPM	● ● ●	●	●

● / ○ : Addressed/Not Addressed, ? : No details provided, - : Not applicable

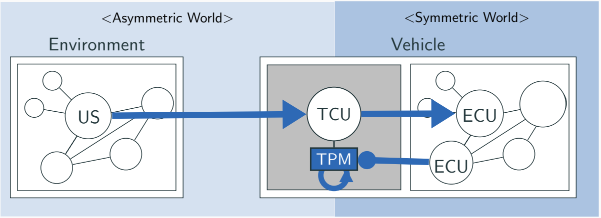
SW: Software-based TCB, M-SW: Measured Software-based TCB (e.g., measured boot)

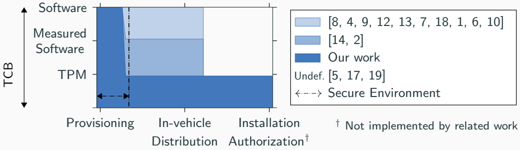


† Not implemented by related work

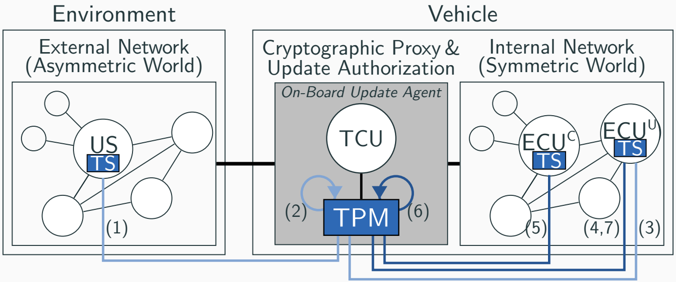
Conclusion

- Secure OTA software update concept for connected vehicles
  - Trusted Platform Module 2.0 (TPM 2.0) as central trust anchor
- Compliant to recent automotive standards and regulations
- Minimize TCB on update agent to just the TPM2.0
- 2 Security Building Blocks
  - Secure transmission with rekeying
  - Installation coordination





Thank you! Questions?



Literature References i

[1] Ali Dorri et al. "BlockChain: A Distributed Solution to Automotive Security and Privacy". In: *IEEE Communications Magazine* 55.12 (2017), pp. 119–125. DOI: 10.1109/MCOM.2017.1700879.

[2] Andreas Fuchs, Christoph Krauß, and Jürgen Repp. "Advanced Remote Firmware Upgrades Using TPM 2.0". In: *ICT Systems Security and Privacy Protection*. Ed. by Jaap-Henk Hoepman and Stefan Katzenbeisser. Cham: Springer International Publishing, 2016, pp. 276–289. ISBN: 978-3-319-33630-5. DOI: 10.1007/978-3-319-33630-5_19.

[3] Andy Greenberg. *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*. URL: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[4] Irina Hossain and Syed Masud Mahmud. "Analysis of a Secure Software Upload Technique in Advanced Vehicles using Wireless Links". In: *2007 IEEE Intelligent Transportation Systems Conference*. Seattle, WA, USA: Institute of Electrical and Electronics Engineers (IEEE), 2007, pp. 1010–1015. DOI: 10.1109/ITSC.2007.4357797.

[5] Muhammad Sabir Idrees et al. "Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates". In: *Communication Technologies for Vehicles)*. Vol. 6596. Oberpfaffenhofen, Germany: Springer, 2011, pp. 224–238. DOI: 10.1007/978-3-642-19786-4_20.

[6] Trishank Kuppusamy, Lois DeLong, and Justin Cappos. "Uptane: Security and Customizability of Software Updates for Vehicles". In: *IEEE Vehicular Technology Magazine* 13 (Feb. 2018), pp. 1–1. DOI: 10.1109/MVT.2017.2778751.

[7] Michele La Manna et al. "Performance Evaluation of Attribute-Based Encryption in Automotive Embedded Platform for Secure Software Over-The-Air Update". In: *Sensors* 21.2 (2021), pp. 1–14. ISSN: 1424-8220. DOI: 10.3390/s21020515. URL: https://www.mdpi.com/1424-8220/21/2/515.

[8] S.M. Mahmud, S. Shanker, and I. Hossain. "Secure software upload in an intelligent vehicle via wireless communication links". In: *IEEE Proceedings. Intelligent Vehicles Symposium, 2005.* Las Vegas, NV, USA: IEEE, 2005, pp. 588–593. DOI: 10.1109/IVS.2005.1505167.

[9] Karim Mansour, Wael Farag, and Mohamed ElHelw. "AiroDiag: A sophisticated tool that diagnoses and updates vehicles software over air". In: *2012 IEEE International Electric Vehicle Conference*. Greenville, SC, USA: IEEE, 2012, pp. 1–7. DOI: 10.1109/IEVC.2012.6183181.

[10] Kathiresh Mayilsamy, Neelaveni Ramachandran, and Vismitha Sunder Raj. "An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air". In: *Computers & Electrical Engineering* 71 (2018), pp. 578–593. ISSN: 0045-7906. DOI: 10.1016/j.compeleceng.2018.08.002. URL: https://doi.org/10.1016/j.compeleceng.2018.08.002.

[11] Microsoft. *Image Gallery*.

[12] D. K. Nilsson and U. E. Larson. "Secure Firmware Updates over the Air in Intelligent Vehicles". In: *ICC Workshops - 2008 IEEE International Conference on Communications Workshops*. Beijing, China: IEEE, 2008, pp. 380–384. DOI: 10.1109/ICCW.2008.78.

[13] Dennis K. Nilsson, Lei Sun, and Tatsuo Nakajima. "A Framework for Self-Verification of Firmware Updates over the Air in Vehicle ECUs". In: *2008 IEEE Globecom Workshops*. New Orleans, LA, USA: IEEE, 2008, pp. 1–5. DOI: 10.1109/GLOCOMW.2008.ECP.56.

[14] Richard Petri et al. "Evaluation of Lightweight TPMs for Automotive Software Updates over the Air". In: *Proceedings of the 4th International Conference on Embedded Security in Cars USA*. Detroit Metropolitan, USA: Escar, 2016, pp. 1–15. DOI: 10.24406/publica-fhg-394900.

[15] Christian Plappert and Andreas Fuchs. "Secure and Lightweight Over-the-Air Software Update Distribution for Connected Vehicles". In: *Proceedings of the 39th Annual Computer Security Applications Conference*. ACSAC '23. Austin, TX, USA: Association for Computing Machinery, 2023. ISBN: 9798400708862. DOI: 10.1145/3627106.3627135. URL: https://doi.org/10.1145/3627106.3627135.

[16] Christian Plappert et al. "Evaluating the applicability of hardware trust anchors for automotive applications". In: *Computers & Security* 135 (2023), p. 103514. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103514. URL: https://www.sciencedirect.com/science/article/pii/S0167404823004248.

[17] Marco Steger et al. "An Efficient and Secure Automotive Wireless Software Update Framework". In: *IEEE Transactions on Industrial Informatics* 14.5 (2018), pp. 2181–2193. DOI: 10.1109/TII.2017.2776250.

[18] Marco Steger et al. "Generic framework enabling secure and efficient automotive wireless SW updates". In: *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. Berlin, Germany: IEEE, 2016, pp. 1–8. DOI: 10.1109/ETFA.2016.7733575.

Literature References iii

[19] Marco Steger et al. "Secure wireless automotive software updates using blockchains: A proof of concept". In: *Advanced Microsystems for Automotive Applications 2017: Smart Systems Transforming the Automobile (Lecture Notes in Mobility*. Ed. by G Meyer, B Muller, and C Zachaus. Switzerland: Springer, 2018, pp. 137–149. DOI: 10.1007/978-3-319-66972-4_12. URL: https://eprints.qut.edu.au/131752/.

[20] Daniel Zelle et al. "ThreatSurf: A method for automated Threat Surface assessment in automotive cybersecurity engineering". In: *Microprocessors and Microsystems* 90 (2022), p. 104461. ISSN: 0141-9331. DOI: https://doi.org/10.1016/j.micpro.2022.104461. URL: https://www.sciencedirect.com/science/article/pii/S0141933122000321.