Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences
Department Informatik

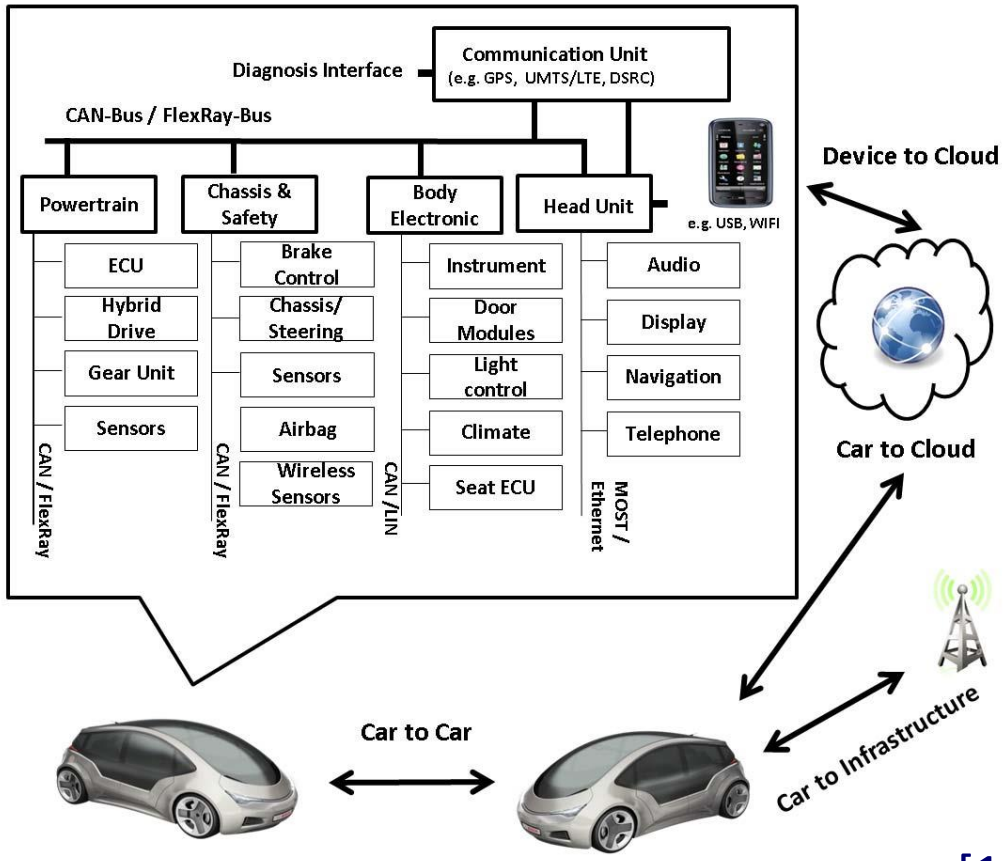
Sicherheitsarchitekturen für automotive Systeme

Jonas Schäufler
12.06.2018

Inhaltsübersicht

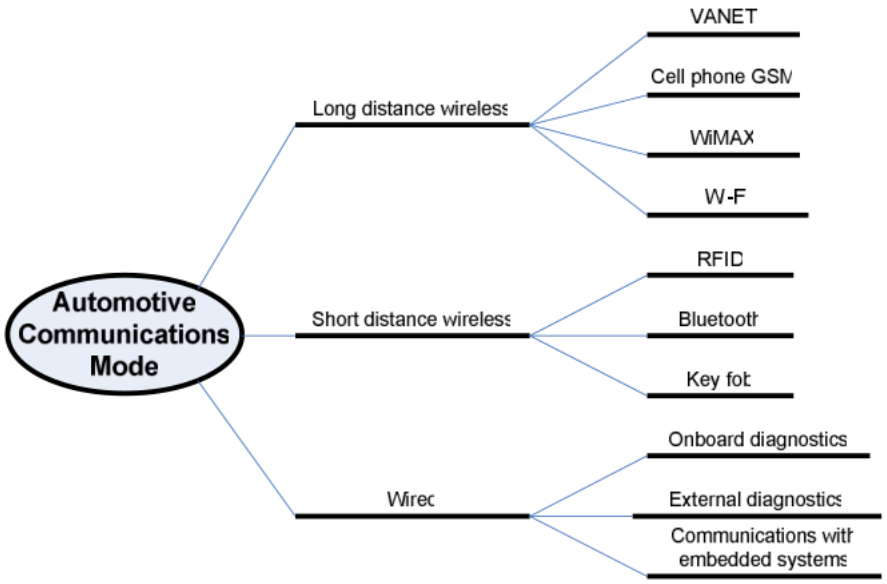
1. Automotive Systeme
2. Sicherheitsarchitektur
3. Forschungsfragen
4. Vorgehensweise
5. Risiken
6. Konzepte
7. Ausblick

IVN Communication



[1]

V2X Communication

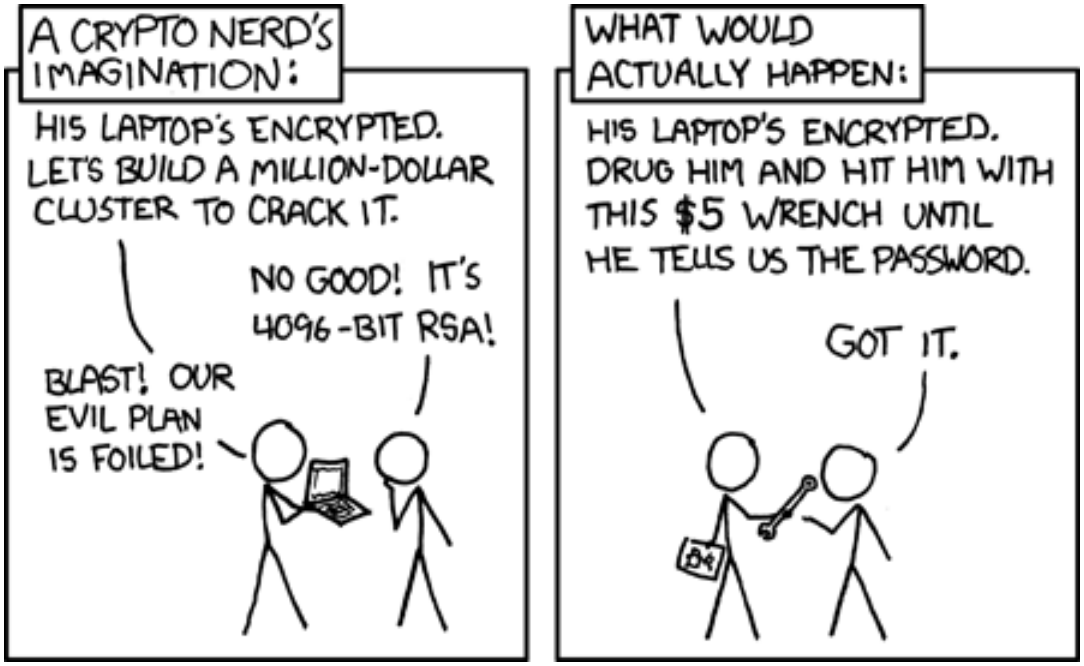


[3]

Schwierigkeiten

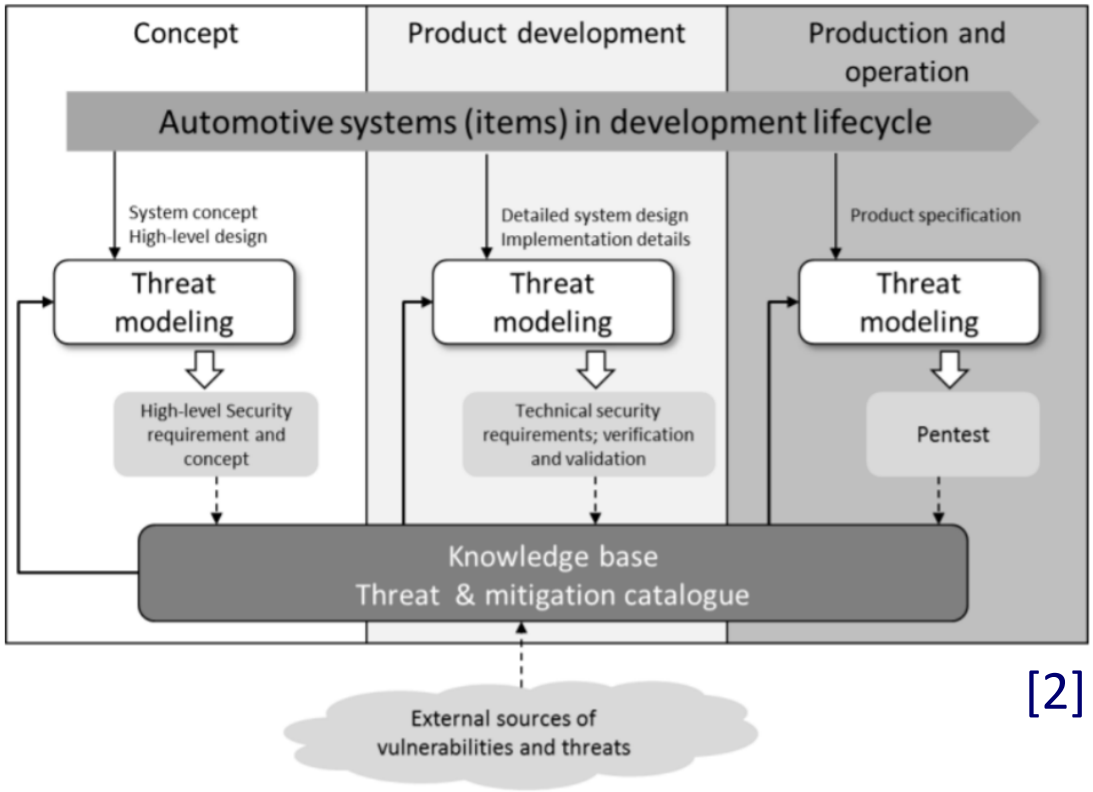
- hohe In-Field Lifetime
- verschiedene Designer, Hersteller, Zulieferer
- Time-to-Market sehr kurz
- Zahlreiche neue Technologien
- „Einfacher“ Physischer Zugang
- Plug & Play
- Limitierte Resourcen
- Harte Constraints

Der Weg zur Sicherheitsarchitektur



[6]

Threat Model



[2]

Nichtfunktionale Anforderungen an eine Sicherheitsarchitektur für automotive Systeme [4]

- Anpassbar
- Verteilt
- Erweiterbar
- Multilevel

Standards in der Entwicklung von Automotive Systemen

- AUTOSAR
- ISO 9001
- IEC-61508
- ISO 26262
- Automotive SPICE

Secure Hardware Extension (SHE):

- Spezifikation
- Definiert API einer ‚Secure Zone‘
- Key Management
- Encapsulating Authentication
- Encryption / Decryption

E-Safety Vehicle Intrusion Protected Applications (EVITA):

- Guidelines für Design, Verifikation und Prototyping verschiedener Sicherheitsarchitekturen für ECUs
- Definiert Funktionalität in drei verschiedenen Sicherheitsstufen (low – high)
- Management von Schlüsseln
- Encryption und Decryption Operationen

Preparing Secure Vehicle-to-X Communication Systems (PRESERVE)

- Baut auf EVITA auf
- Ziel ist es ein Subsystem für V2X Anwendungen zu Entwickeln, Implementieren und zu Testen
- Sichere übertragung von Daten- und Steuernachrichten
- Hardware Sicherheitsmodul mit Elliptic Curve Cryptography (ECC)

Forschungsfragen

- Wie muss eine Sicherheitsarchitektur für automotive Systeme aussehen?
- Welche Konzepte sind in welchem Teilbereich anwendbar?
- In welcher Form lassen sich neue Konzepte und Technologien in vorhanden Strukturen integrieren?

Vorgehensweise

Grundprojekt:

„Bestandsaufnahme“ neuer Konzepte / Technologien und Überprüfung auf Anwendbarkeit im automotive Bereich.

Hauptprojekt:

Implementierung eines ausgewählten Konzeptes.

Masterarbeit:

Validierung / Auswertung / Integration in vorhandene Strukturen

Risiken

- Umsetzung fehlerhaft -> Nicht sicher
  (Ziel verfehlt)
- Nicht anwendbar
- Fehleinschätzung des Aufwandes

Konzepte

- Location-enhanced authentication using the IoT: because you cannot be in two places at once. [17]
- Automotive Electrical and Electronic Architecture Security via Distributed In-Vehicle Traffic Monitoring. [16]
- Fingerprinting Electronic Control Units for Vehicle Intrusion Detection [15]
- Video-based Face Recognition Technology for Automotive Security [19]
- BlockChain: A Distributed Solution to Automotive Security and Privacy [13]
- Towards viable certificate-based authentication for the internet of things. [21]
- An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars [20]

Weitere Ansätze

Ausnutzen neuer Hardware:

- **Drive PX Pegasus:**
  - 16 NVIDIA Custom Carmel ARM64
  - 2x Volta iGPU (512 CUDA cores)
  - 2x post-Volta dGPUs

Secure Microcontrollers

- **ST33GXXX Microcontroller Family:**
  - ARM SC300 32-Bit RISC
  - Hardware security-enhanced DES and AES accelerators
  - Memory protection unit (MPU)
  - Monitoring of environmental parameters
  - 16- and 32-bit CRC calculation
  - True random number generator
  - NESCRYPT coprocessor for public key cryptography algorithm

Quellen

- [1] https://www.renesas.com/en-eu/solutions/automotive/technology/networking.html
- [2] Ma, Zhendong & Schmittner, Christoph. (2016). Threat Modeling for Automotive Security Analysis. 333-339. 10.14257/astl.2016.139.68.
- [3] R. R. Brooks, S. Sander, J. Deng, and J. Taiber. 2008. Automotive system security: challenges and state-of-the-art. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08), Frederick Sheldon, Axel Krings, Robert Abercrombie, and Ali Mili (Eds.). ACM, New York, NY, USA
- [4] Camek, Alexander et al. “Future cars: necessity for an adaptive and distributed multiple independent levels of security architecture.” *HiCoNS* (2013).
- [5] Soja, Richard. “Automotive Security: From Standards to Implementation.” (2014).
- [6] https://xkcd.com/538/
- [7] Bassem Mokhtar, Mohamed Azab, Survey on Security Issues in Vehicular Ad Hoc Networks, Alexandria Engineering Journal, Volume 54, Issue 4, (2015)
- [8] McAfee: Automotive Security Best Practices: Recommendations for security and privacy in the era of the next-generation car.
- [9] W. Yan, "A two-year survey on security challenges in automotive threat landscape," *2015 International Conference on Connected Vehicles and Expo (ICCVE)*, Shenzhen, 2015, pp. 185-189.

Quellen

- [10] H. Yu and C. W. Lin, "Security concerns for automotive communication and software architecture," *2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, San Francisco, CA, 2016, pp. 600-603.
- [11] P. Waszecki, P. Mundhenk, S. Steinhorst, M. Lukasiewycz, R. Karri and S. Chakraborty, "Automotive Electrical and Electronic Architecture Security via Distributed In-Vehicle Traffic Monitoring," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 11, pp. 1790-1803, Nov. 2017.
- [12] R. Rieke, M. Seidemann, E. K. Talla, D. Zelle and B. Seeger, "Behavior Analysis for Safety and Security in Automotive Systems," *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, St. Petersburg, 2017, pp. 381-385.
- [13] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," in *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119-125, 2017
- [14] Ray, S., Chen, W., Bhadra, J., & Faruque, M.A. (2017). Extensibility in Automotive Security: Current Practice and Challenges: Invited. *DAC*.
- [15] Cho, Kyong-Tak and Kang G. Shin. “Fingerprinting Electronic Control Units for Vehicle Intrusion Detection.” *USENIX Security Symposium* (2016).

Quellen

- [16] P. Waszecki, P. Mundhenk, S. Steinhorst, M. Lukasiewycz, R. Karri and S. Chakraborty, "Automotive Electrical and Electronic Architecture Security via Distributed In-Vehicle Traffic Monitoring," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 36, no. 11, pp. 1790-1803, Nov. 2017.
- [17] Ioannis Agadakos, Per Hallgren, Dimitrios Damopoulos, Andrei Sabelfeld, and Georgios Portokalidis. 2016. Location-enhanced authentication using the IoT: because you cannot be in two places at once. In Proceedings of the 32nd Annual Conference on Computer Security Applications (ACSAC '16). ACM, New York, NY, USA, 251-264. DOI: https://doi.org/10.1145/2991079.2991090
- [18] AUTOSAR CP Release 4.3.1: Specification of Secure Onboard Communication
- [19] RongBao Chen and ShiJie Zhang, "Video-based face recognition technology for automotive security," *2010 International Conference on Mechanic Automation and Control Engineering*, Wuhan, 2010, pp. 2947-2950.
- [20] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars," *2015 Sixth International Conference on Emerging Security Technologies (EST)*, Braunschweig, 2015, pp. 86-91.
- [21] René Hummen, Jan H. Ziegeldorf, Hossein Shafagh, Shahid Raza, and Klaus Wehrle. 2013. Towards viable certificate-based authentication for the internet of things. In Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy (HotWiSec '13). ACM, New York,