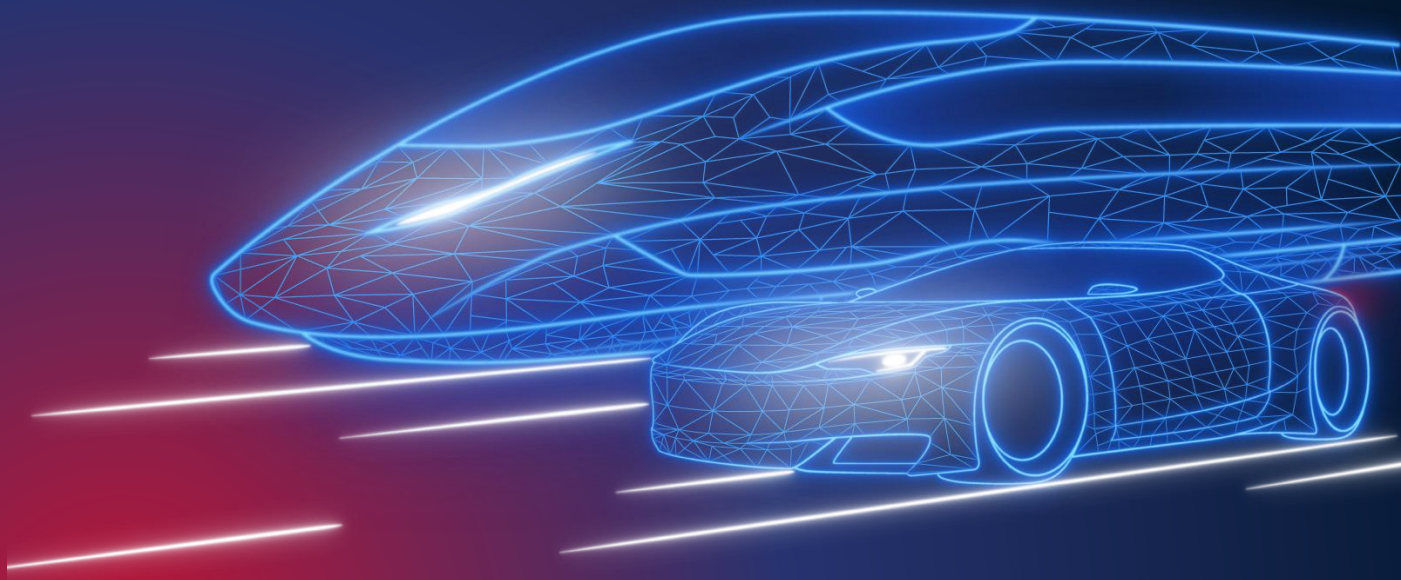
YEKTA IT

INCYDE



VATT&EK: Formalization of Cyber Attacks on Intelligent Transport Systems – a TTP based approach for Automotive and Rail

7th ACM Computer Science in Cars Symposium (CSCS '23), December 05, 2023, Darmstadt, Germany

Ali Recai Yekta , Dominik Spychalski, Erhan Yekta, Cenk Yekta, Stefan Katzenbeisser

Content

1. Project background
2. Motivation
3. VATT&EK Framework
   - in Automotive
   - in Railway
   - Use Cases
4. Conclusion & Outlook

Project background
VATT&EK Framework

FINESSE

Vehicle intrusion detection and prevention in a standardized structure for road and rail

- Development of a multi-modal and **holistic security monitoring system for vehicles**
- Joint consideration of **road and rail vehicles** to identify and utilize synergy effects
- Conception and definition of a **standardized security architecture**
- Design, implementation and testing of secure on-board components to **detect vehicle-specific attacks** as well as scaling attacks on vehicle fleets, groups or communication channels (backend analytics)
- **We discovered: Common attack formalization models have reached their limits** when it comes to ITS security monitoring at all architectural levels
  - We need a holistic understanding of attack vectors and attack behavior on ITS
  - We need a holistic understanding of vehicle architectures and the attack phases on each architecture level
  - There was a need for a common and sound taxonomy! → VATT&EK

SPONSORED BY THE
Federal Ministry of Education and Research

Consortium:

DB eTAS Fraunhofer SIT INCYDE UNIVERSITÄT PASSAU YEKTA IT

More FINESSE: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/finesse

Motivation
VATT&EK in ITS

Why VATT&EK in ITS?

Current challenges in ITS cybersecurity

- Vehicles once isolated mechanical entities, now complex interconnected systems
- Increasing networking and complexity of ITS
- Increase in targeted cyber attacks on transportation systems → changing and envolving threat landscape
- Difficulties in securing heterogeneous and distributed systems.
- There was a need for a common and sound taxonomy! → VATT&EK

Limitations of existing attack formalization frameworks

- Frameworks such as **MITRE ATT&CK** are mostly geared towards **traditional IT environments**
- **Gaps related to automotive attack frameworks**
- **No framework for rail transport available**
- **Lack of specific tools and strategies** for the **unique ITS threat landscapes**.

There is a need for a customized framework that directly addresses the specific security requirements of ITS!

Methodology

Methodology

- Analyzing the principles of existing attack formalization frameworks (MITRE ATT&EK, Auto ISAC, ASRG)
  - identify gaps
  - Integrated them (tactics, techniques, …) into the ITS domain, if suitable
- Decade-long retrospective analysis of automotive cyber attacks
  - Classify attacks and identify attack phases
  - Discern the techniques utilized
  - Subsequently refine VATT&EK Framework
- To ensure a holistic understanding, we engaged with experts from OEMs (in the paper indicated as [OI]) enriched with insights from security professionals and penetration testers (in the paper indicated as [PTE])

The VATT&EK Framework

Basics and structure

Tactics

The strategic goals or intentions of an attacker, e.g. "gaining access to the vehicle"

Techniques

The specific techniques or approaches used by attackers, e.g. "Exploitation of WiFi Stack"

Procedure

The exact steps or actions that an attacker takes, e.g. "Code Execution in WiFi Chip"

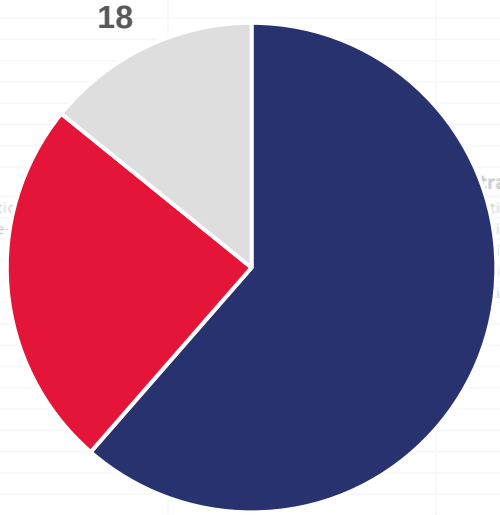
Expert Knowledge

Collaboration with OEMs and security professionals.

VATT&EK Tactics & Techniques

Manipulate Environment	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Downgrade Attacks via Rogue Base stat	Radio Data System (RDS) Attacks	Command and Scripting Interprete	Persistence via Credentials	Exploit Application Vulnerability	Bypass SecurityAccess	Adversary-in-the-Middle	ECU Discovery
Rogue Cellular Base Station	Malicious SMS	Inter-process Communication: D-B	Firmware Installation - Reprogram ECU	Exploit OS Vulnerability	Bypass Code Signing Check	Brute Force	ECU Service Discovery
Rogue Wi-Fi Access Points	Exploitation of Wi-Fi Stack	Native API	Modify OS Kernel, Boot / System P		Firmware Installation - Reprogram ECU: Downgra	Input Capture	Network Service Scanning
GNSS Attacks	Gain access to Wi-Fi Hotspot	Scheduled Task/Job	Modify TEE		Deactivate Immobilizer	SMS Message Capture	Network Sniffing
GNSS Spoofing Attacks	Exploitation via Bluetooth	User Execution		Reprogram ECU for privilege escalati	Downgrade to insecure protocol	Network Sniffing	
GNSS Jamming	Exploitation via C-V2X				Enable Remote Functions	OS Credential Dumping	
Sybil Attack	Exploitation via DSRC					Unsecured Credentials	
Camera Attacks	Exploitation via Repair Shop/Garage/Factory					Exploit TEE Vulnerability	
General Attacks on Camera Systems	Exploitation of OBD Dongles						
Camera Feature Attacks	Hardware addition						
Blinding the Camera	Physical Access (CAN-Injection)						
LiDAR Attacks	Connect						
LiDAR Replay Attacks	Code Execution via USB						
LiDAR Relaying Attack	Code Execution via SD Card						
LiDAR Spoofing Attacks	Code Execution via	Lateral Movement	Collection		ration	Affect Vehicle Function	Impact
LiDAR Jamming/Saturation Attack	Exploitation via OBD Interface	Exploitation of Remote Services	Gather informatio		ion via Memory mapped Registers	Control Horn	Denial of Control
Spoofing FMCW Radar	Supply Chain Com	Pass the Ticket	Adversary-in-the		ion via Removable Media	Control HVAC	Denial of View
Black Hole Attacks	Unsecured Web A	Replication Through Removable M	Audio Capture		ion via SMS	Control Engine	Loss of Control
TPMS Attacks	Hacking in-vehicle apps	Exploit EDI for Lateral Movement	Input Capture		ion via C-V2X	Control Doors	Enable premium features
TPMS Jamming	Malicious App Delivery		Screen Capture		ion via DSRC	Control Lights	Chip Tuning
TPMS Spoofing	Drive-by Compromise		Video Capture			Control Airbag	Odometer fraud
Attacks on Road Side Units/Balise	Exploitation via charging station					Control Windows	Vehicle Theft
	Keyless Go Attacks					Speed control	
	Replay Attack					Speed control via Radio	
	Relay Attack					Send halt signal via Radio	
	Roll Jam Attack					Manipulate Passenger Information System	
	Roll Back Attack					Control Instrument Panel Cluster (IPC)	
	Service Compartment Access					Denial of Service	
	Maintenance Notebook Infection					Message Injection	
	Exploitation of Internet Accessible Device					Control Brake	
	Remote Maintenance Accesspoint						

Techniques



VATTEK MITRE AutoISAC

VATT&CK consists of:

- **14** tactics
- **127** techniques
- thereof **78 new**

VATT&EK in Automotive

Jeep Hack 2015: "Researchers hacked a vehicle via the multimedia system and gained control over important functions."

- Identification of the **tactic** Initial Access: "Gain remote access to vehicle systems"
- Analysis of the **technique**: "Exploitation of Internet Accessible Device"
- Investigation of the **procedure**: "Brute force attack on the Wi-Fi password, followed by firmware manipulation to control the vehicle."
- ***remote attack chain:*** Exploitation of Internet Accessible Device → Inter-process Communication → Reprogram ECU for privilege escalation → (Control Lights | Kill Engine | Control IPC | Control Brake)

VATT&EK in Railway

Hackers use radio signals to bring over 20 trains to a standstill in a cyber attack on the rail network in Poland.

- Analysis of a **real cyberattack** on trains in Poland.
- Identification of the **tactic** Affect Vehicle Function: "Disrupt train traffic" Analysis of the **technique**: "Use of a simple radio hack"
- Investigation of the **procedure**: "Sending radio signals to trigger an emergency stop"
- Such mapping cannot be represented with frameworks such as MITRE ATT&CK

Poland investigates cyber-attack on rail network

26 August

Russia-Ukraine war

Some trains were brought to a standstill for a few hours

Use Cases

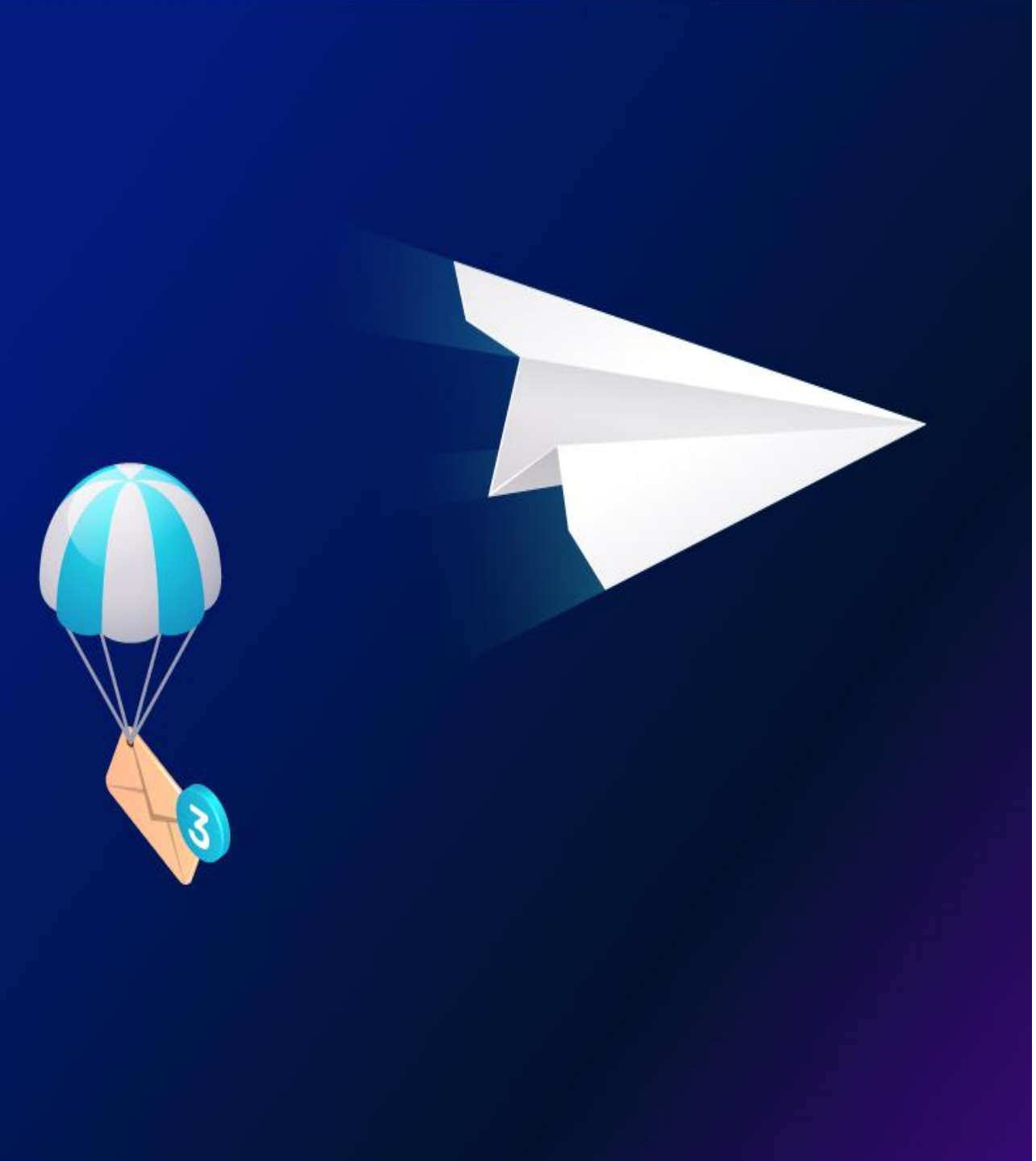
TARA support	•Systematic threat pinpointing and prioritization •Enabling precise risk assessments and targeted mitigation strategies for vehicle cyber security
Penetration Testing Roadmap	•How can I test a vehicle or vehicle components systemically? •What are possible attack vectors?
Threat Intelligence	•Manual / automated cyber attack analyses and mapping to techniques •Improved tracking of different reports
Security Monitoring	•What are reasonable security monitoring use cases for vehicles? •How large is the SuC/Use Case coverage?
Incident Response	•How did the attacker get access? What other traces are there? •Dashboard for visualization
Teaching & Research	•Gain understanding of different cyber attack tactics, techniques, and their interplay •Common taxonomy to discuss ITS related cyber attacks and to fosters collaboration

Conclusion & Outlook

- VATT&EK addresses specific cybersecurity challenges in ITS.
- VATT&EK was developed based on real scenarios in the automotive and rail transport industries
- VATT&EK will adapt to future technological developments such as autonomous driving
- **VATT&EK offers a comprehensive and flexible approach to ensure safety in the ever-evolving world of Intelligent Transportation Systems.**

VATT&EK closes a gap on ITS attack formalization

- VATT&EK provides a Roadmap for ethical hackers
- VATT&EK provides a **structured approach to understand**, visualize and address ITS cyber threats
- VATT&EK **Improves threat detection** and response in ITS
- VATT&EK **increases the overall security** and reliability of transportation systems



Questions or impulses?

Ali Recai Yekta

Yekta IT GmbH

ali@yekta-it.de

www.yekta-it.de

Dominik Spychalski

INCYDE industrial cyber defense GmbH

dominik.spychalski@incyde.com

www.incyde.com

Findings, paper & more (soon):

vehicle-threat-matrix.com

Appendix

VATT&EK - Tactics

- ATA_1 Manipulate Environment (ME)
- ATA_2 Initial Access (IA)
- ATA_3 Execution (EX)
- ATA_4 Persistence (PS)
- ATA_5 Privilege Escalation (PE)
- ATA_6 Defense Evasion (DE)
- ATA_7 Credential Access (CA)
- ATA_8 Discovery (DS)
- ATA_9 Lateral Movement (LM)
- ATA_{10} Collection (CL)
- ATA_{11} Command and Control (C2)
- ATA_{12} Exfiltration (EF)
- ATA_{13} Affect Vehicle Function (AF)
- ATA_{14} Impact (IM

ATA_2 Initial Access (IA)

- ATE_1 *RDS Attacks*
- ATE_2 *Malicious SMS*
- ATE_3 *Exploitation of Wi-Fi Stack*
- ATE_4 *Gain access to Wi-Fi Hotspot*
- ATE_5 *Exploitation via Bluetooth*
- ATE_6 *Exploitation via C-V2X*
- ATE_7 *Exploitation via DSRC.*
- ATE_8 *Exploitation via Repair Shop/Garage/Factory*
- ATE_9 *Exploitation of OBD Dongles*
- $ATE_{10.1}$ *Hardware Addition (CAN-Injection)*
- ATE_{11} *Exploitation via OBD Interface*
- ATE_{12} *Supply Chain Compromise*
- ATE_{13} *Unsecured Web APIs*
- ATE_{14} *Hacking in-vehicle apps*
- ATE_{15} *Malicious App Delivery.*
- ATE_{16} *Drive-by Compromise.*
- ATE_{17} *Exploitation via charging station*
- ATE_{18} *Keyless Go Attacks*
- ATE_{19} *Service Compartment Access*
- ATE_{20} *Maintenance Notebook Infection*
- ATE_{21} *Exploitation of Internet Accessible Device*
- ATE_{22} *Remote Maintenance Accesspoint*

Chaining Tactics

- ATA_3 Execution (EX)
- ATA_4 Persistence (PS)
- ATA_5 Privilege Escalation (PE)
- ATA_6 Defense Evasion (DE)
- ATA_7 Credential Access (CA)
- ATA_8 Discovery (DS)
- ATA_9 Lateral Movement (LM)
- ATA_{10} Collection (CL)
- ATA_{11} Command and Control (C2)
- ATA_{12} Exfiltration (EF)

ATA_{13} Affect Vehicle Functions

- ATE_1 *Control Horn:*
- ATE_2 *Control HVAC*
- ATE_3 *Control Engine*
- ATE_4 *Control Doors*
- ATE_5 *Control Lights*
- ATE_6 *Control Airbag*
- ATE_7 *Control Windows.*
- ATE_8 *Speed control.*
- ATE_9 *Speed control via*
- ATE_{10} *Stop Vehicle via Radio*
- ATE_{11} *Manipulate Passenger Information System*
- ATE_{12} *Control Instrument Panel Cluster*
- ATE_{13} *Denial of Service (DoS)*
- ATE_{14} *Message Injection*
- ATE_{15} *Control Brake*

ATA_{14} Impact (IM)

- ATE_1 ***Denial of Control.*** Attackers disrupting a vehicle's control systems, preventing operators
- ATE_2 ***Denial of View.*** Attackers obscure or manipulate the data presented to vehicle operators
- ATE_3 ***Loss of Control.*** Attackers seize control of specific vehicle functions, overriding operator inputs
- ATE_4 ***Enable premium features***. Attackers unlock features that are typically behind a paywall or not activated
- ATE_5 ***Chip Tuning.*** This refers to the modification of the ECU to enhance a vehicle's performance, potentially compromising safety standards and regulatory compliances.
- ATE_6 ***Odometer fraud.*** Attackers manipulate the vehicle's odometer readings, typically to reduce the displayed mileage, affecting the vehicle's resale value and potentially misleading buyers about its usage history.
- ATE_7 ***Vehicle Theft***. Attackers leveraging cyber vulnerabilities to bypass security measures and steal the vehicle, which can be applicable to both vehicles and specialized rail equipment.

Evaluation

Jeep Hack 2015:

remote attack chain: Exploitation of Internet Accessible Device → Inter-process Communication → Reprogram ECU for privilege escalation → (Control Lights | Kill Engine | Control IPC | Control Brake)

BMW Hack 2015:

remote attack chain: Rogue Wi-Fi Access Points → Malicious SMS → Enable Remote Functions → Malicious SMS → Control doors

CAN Injection Attack 2023:

local attack chain: Hardware Addition (CAN Injection) → Message Injection → Control Doors → Deactivate Engine Immobilizer