IT-SECURITY FOR E-MOBILITY

Prof. Dr. Christoph Krauß

IDC 2019, Scientific School

October 9th, 2019

St. Petersburg, Russia

Fraunhofer SIT

Member of CRISP Center for Research in Security and Privacy

Fraunhofer Institute for Secure Information Technology SIT

Leading Institution for Applied Cybersecurity Research in Germany

Founded: 1961

Employees: 180

Annual budget: 11 m€

Chair at TU Darmstadt: 1

Additional Professorship at TU Darmstadt: 1

Professorships at h_da: 1

Main Locations: 3 (Darmstadt, Birlinghoven, Mittweida)

Additional locations: 2 (Jerusalem, Singapore)

Fields of Expertise

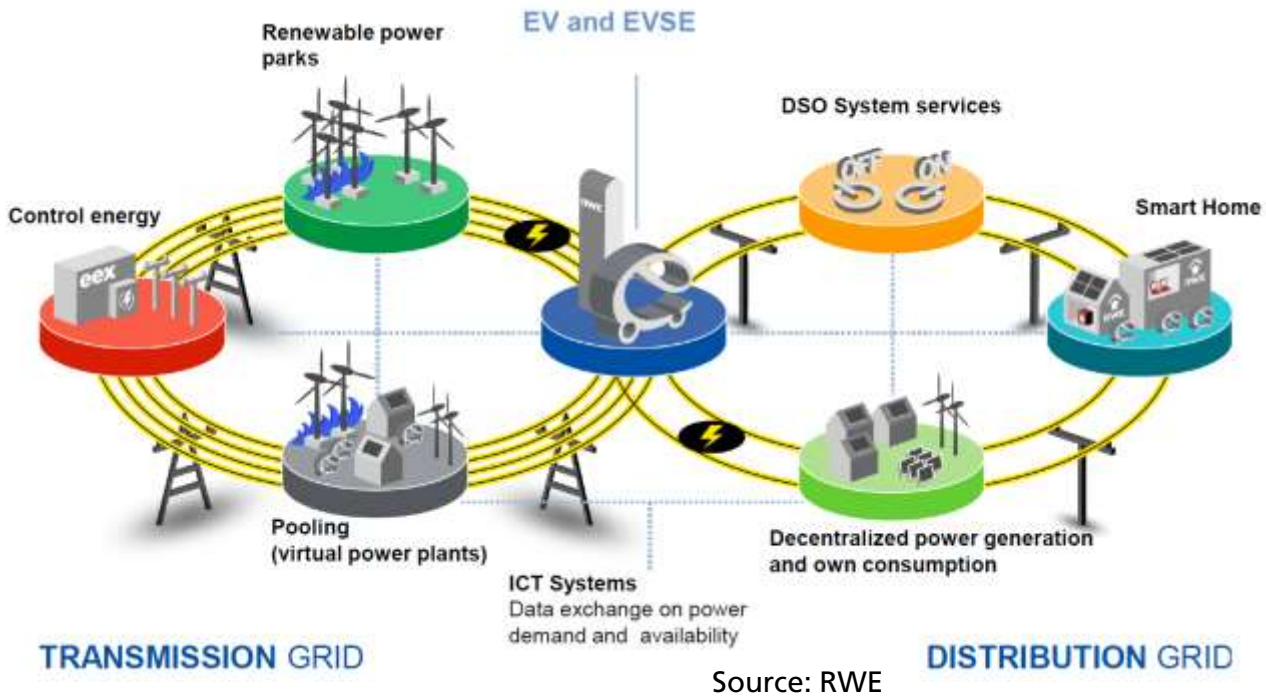
- Automotive Security
- Cloud Computing
- Cyber-Physical Systems
- Identity & Privacy
- Industry 4.0
- Mobile Systems & Networks
- Secure Engineering
- Security Management
- Security Test Lab
- …

Engaged in

- CRISP
- Fraunhofer-Competence Centre “Privacy & Data Protection in the Digital World”
- Learning Laboratory Cybersecurity
- Digital Hub Cybersecurity Darmstadt

Introduction

- Electric mobility is an important technology to reduce emissions in cities
- European Commission developed a roadmap with initiatives towards a competitive and resource efficient transport system
  - By 2030, reduce transport emissions by 20% and only 50% conventionally-fueled cars in cities
  - By 2050, reduce transport emissions by 60% and no conventionally-fueled cars in cities
- Electric mobility will play a major role in the future smart grid



Source: RWE

Introduction

- Smart charging drives the energy revolution forward
  - Satisfy user requirements
  - Demand response and load management
  - Vehicle-to-Grid (V2G)
- Information and communication technology (ICT) required
- However, new security and privacy threats arise
  - Threats to (safety-critical) systems
    - Influence the power grid, inject malware to vehicles etc.
  - Monetary threats
    - Charging for free or on the account of someone else
  - Privacy threats
    - Generation of movement profiles

Source: https://thehackernews.com/2017/06/electric-power-grid-malware.html

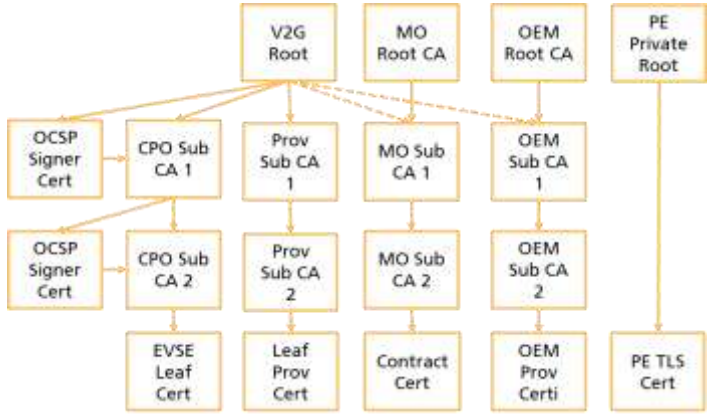
Source: http://ccc.de/en/updates/2017/e-motor

Payment Options

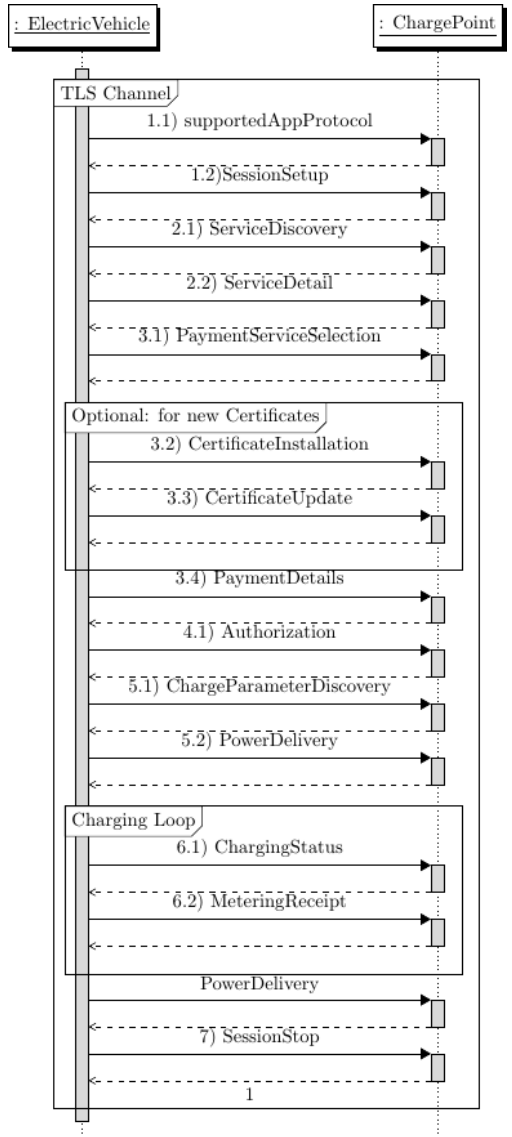
- Charging costs are included in fees for other services
- Cashless payment using EMV reader (not often used)
- External Authentication Means (EIM)
  - (RFID) Charging Card
  - Smartphone App
- Plug and Charge (PnC) using ISO 15118

Charging Card [Entega]

Smartphone App [Fraunhofer SIT]

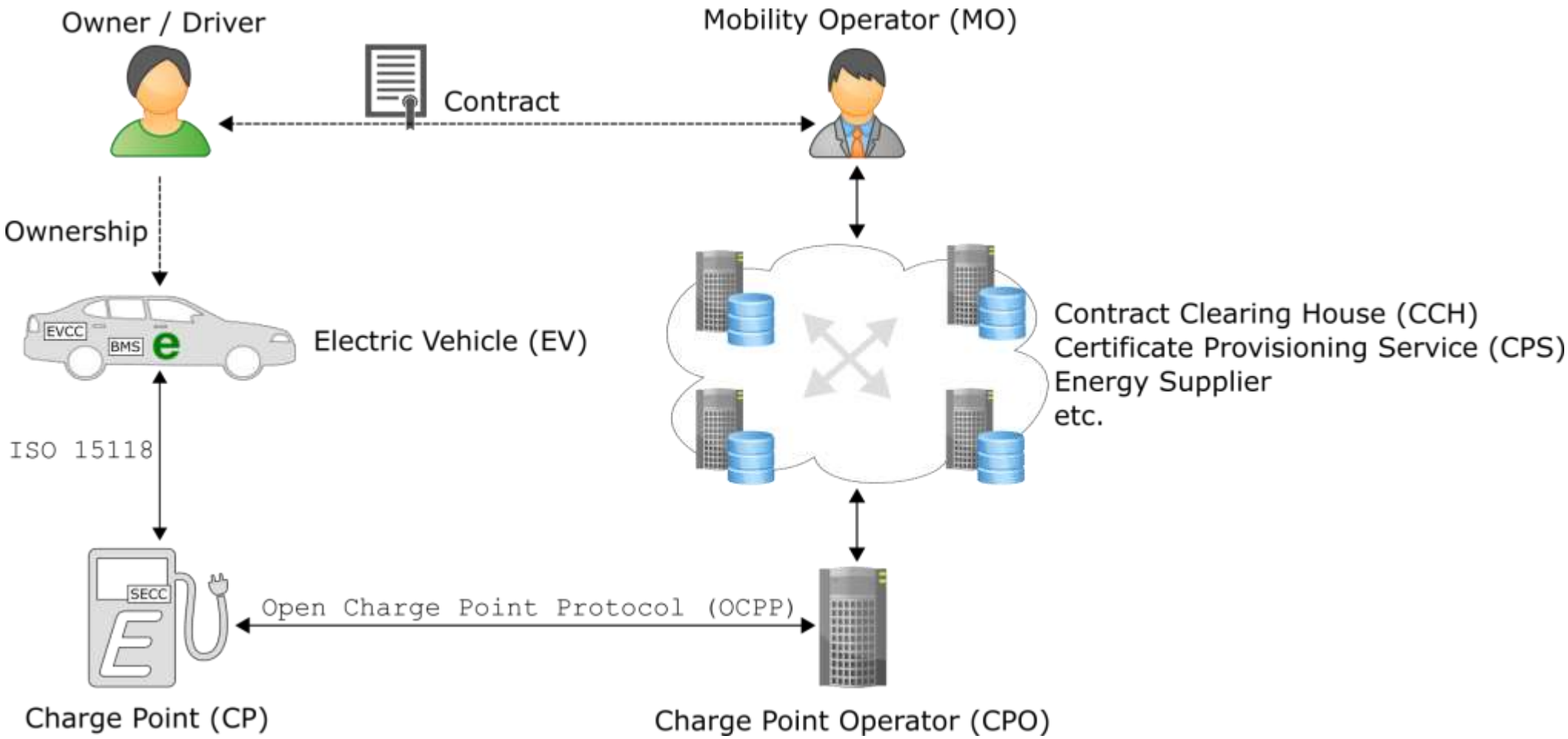


ISO 15118: PKI

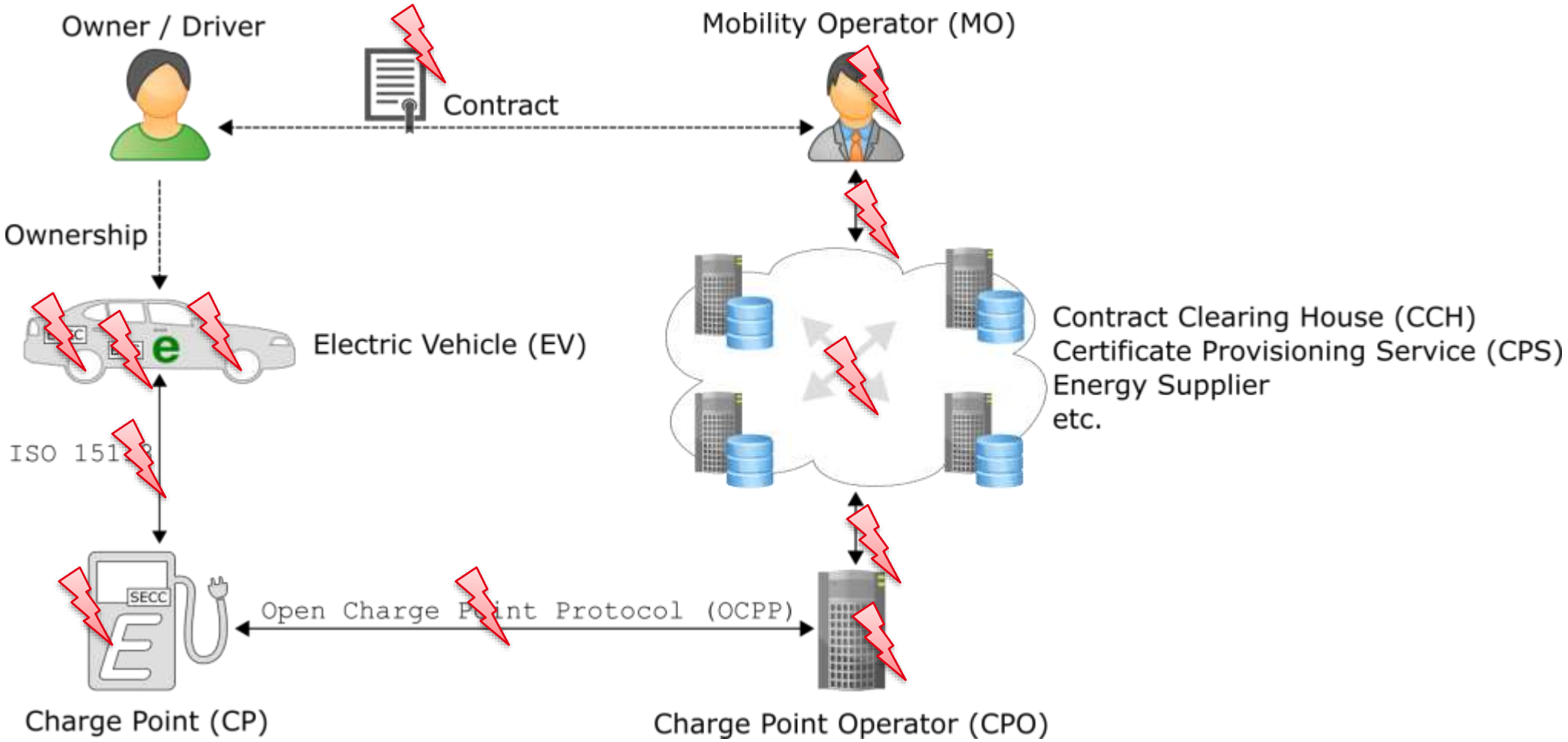


ISO 15118: (TLS) Communication

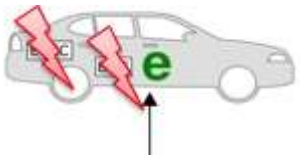
Typical PnC Architecture



IT-Security and Privacy Challenges

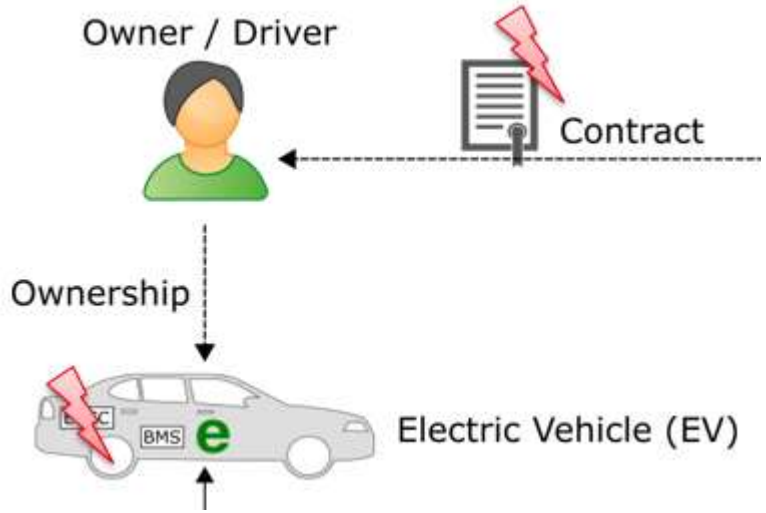


Attacks on Electric Vehicles

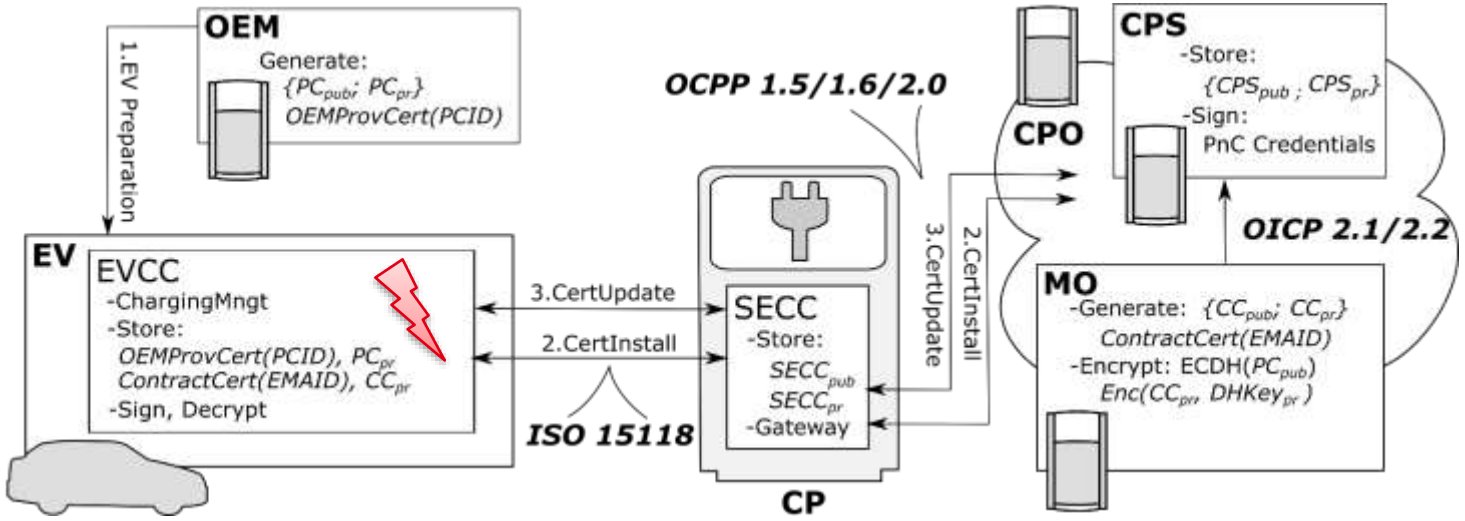


- Electric Vehicles (EVs) could be attacked via communication interfaces or physical access
- Example: Attack of an malicious Charge Point (CP)
  - Data connection between CP and EV could be used for attacks on an EV
    - Data connection examples: PLC in ISO 15118, CAN in CHAdeMo
  - Vulnerabilities in the EV's communication controller could be exploited to
    - Overcharge the batteries
    - Inject messages to the E/E system (if no appropriate separation is deployed)
- By compromising a large number of EVs, attacks on the power grid may be possible, e.g., by influencing the load management

Attacks on ISO 15118 Credentials



- EVs store critical credentials
  - ISO 15118 OEM provisioning certificate and private key
  - ISO 15118 contract certificate and private key
- Currently no requirements for secure key storage and usage



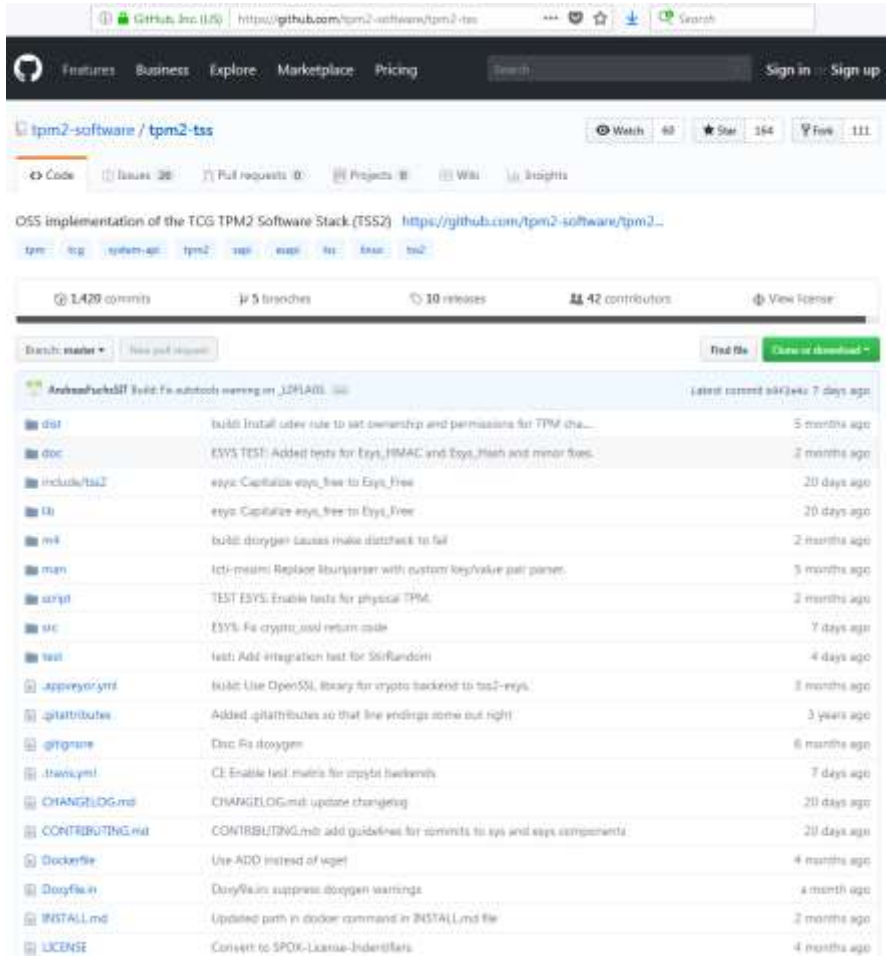
➔ Attacker could easily read out credentials

Trusted Computing – Overview

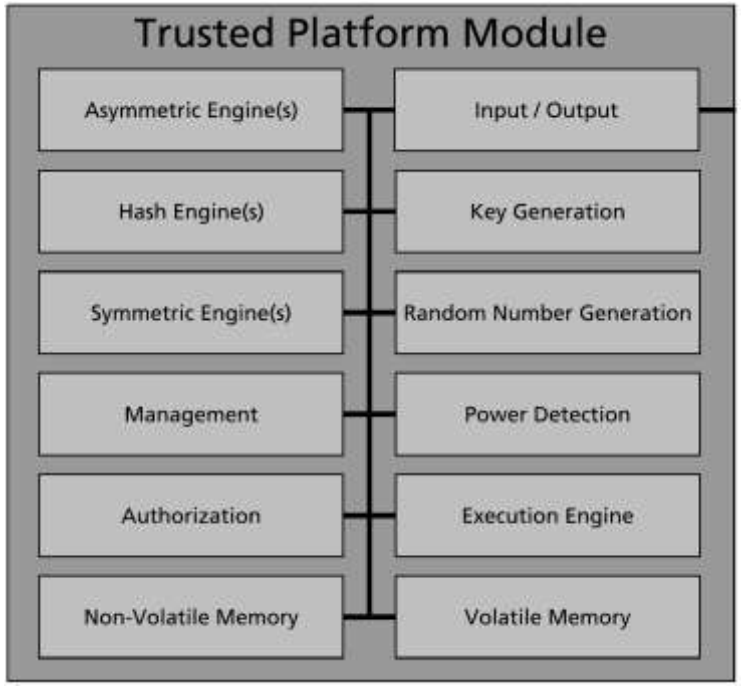
- Hard- and software to enforce that a system behaves consistently and in expected ways
- More than only the Trusted Platform Module (TPM)
  - TPM 2.0 can act as Hardware-Trust-Anchor
  - Hardened against physical attacks
  - Provides secure storage, execution, and more
- Additional Trusted Computing features
  - Measured Boot
  - Attestation
  - Secure device identities …

➔ Trusted Computing as basis for Platform Security

© Infineon

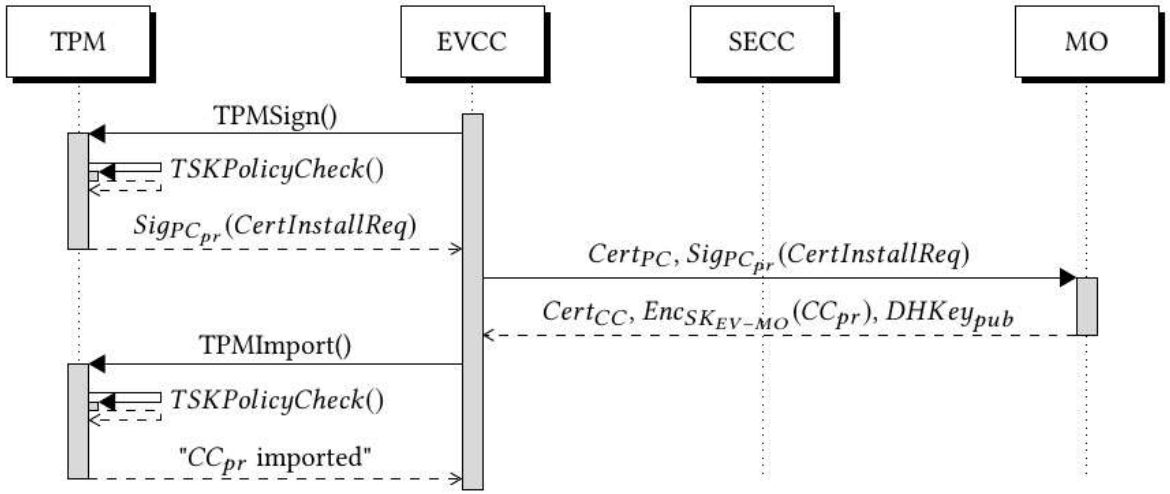


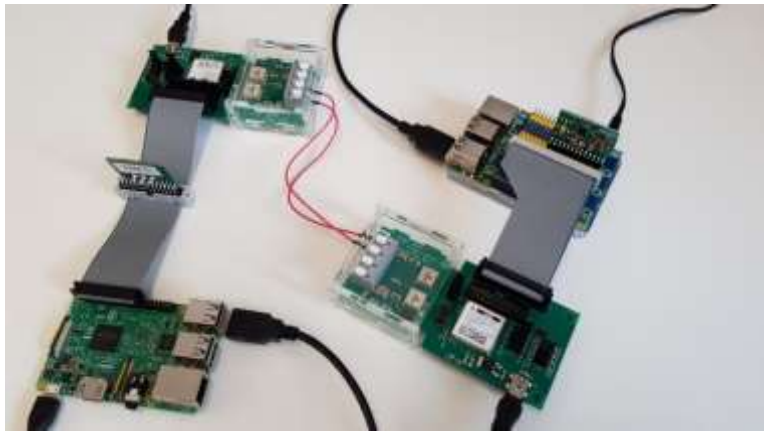
Trusted Platform Module (TPM) – Overview

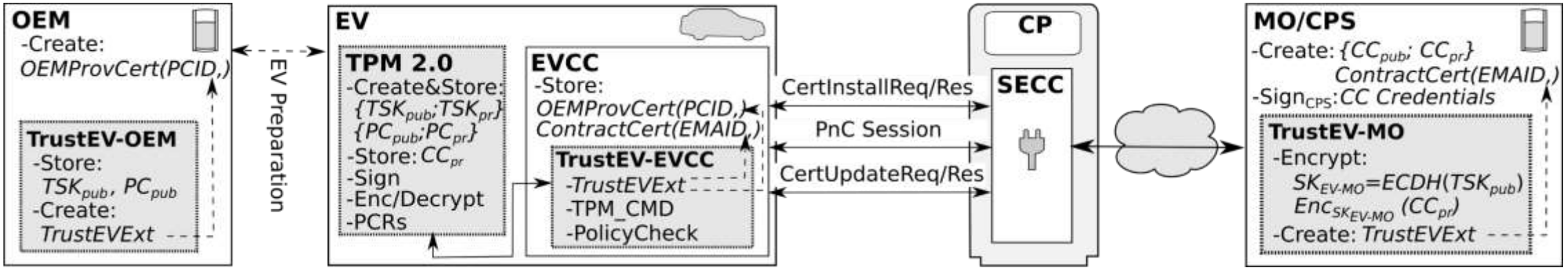


- TPM is a type of Hardware Security Module (HSM)
- Two Specifications: TPM 1.2 and TPM 2.0
  - Specifications are not compatible
  - TPM 2.0 total rewrite and suitable for embedded systems
- Functionalities in Version 2.0
  - Device identification
  - Secure generation, storage, and usage of keys
  - Root of trust for storage, measurement, and reporting
  - Cryptographic agility
  - Enhanced authorization
  - Flexibility (TPM library profiles, dedicated hardware chip vs. firmware TPM …)
  - Encrypted communication between TPM and host or even backend systems
  - Monotonic counters
  - etc.
- Automotive qualified TPMs are available currently from Infineon

Securing ISO15118 Credentials

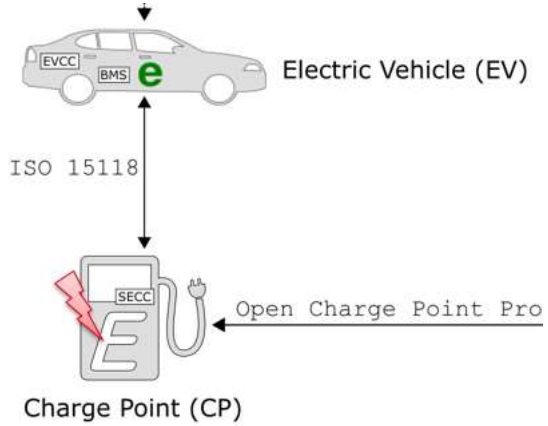




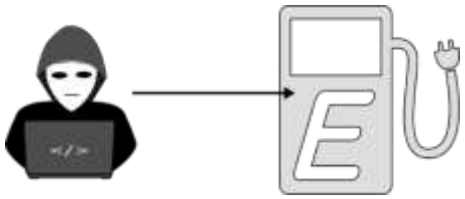


[FKKZ20] A. Fuchs, D. Kern, C. Krauß, M. Zhdanova. TrustEV: Trustworthy Electric Vehicle Charging and Billing, 2020

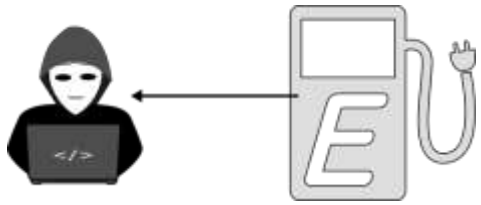
Attacks on Charge Points



- Attacker can attack a CP remotely or via physical access
- CP stores and processes critical data, e.g., (private) keys, billing data, metering data, log data, authorization data, configuration data
- Attacker could …



… manipulate billing data

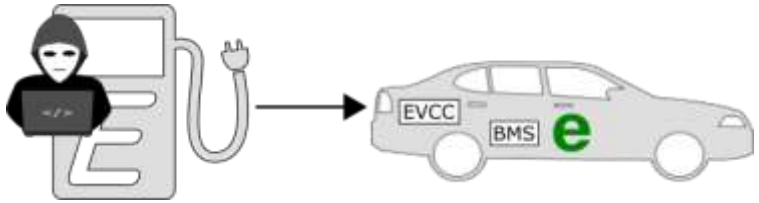


… read out keys and data

… read out personal data

… manipulate firmware

… prevent charging



… attack the vehicle

… and many more, e.g., manipulate the power grid (by compromising a large number of CPs)

Attacks on Charge Points – Examples

- Attacks using insecure maintenance ports
  - Attack on Keba P30 CP [Dal17]
    - Insecure firmware update process via USB enables installation of malicious firmware
- Attack on CP authentication mechanism
  - Fastned / ABB [Dal17]
    - Vehicle MAC address is used for authentication
    - Spoofing of MAC address possible to charge on the account of someone else

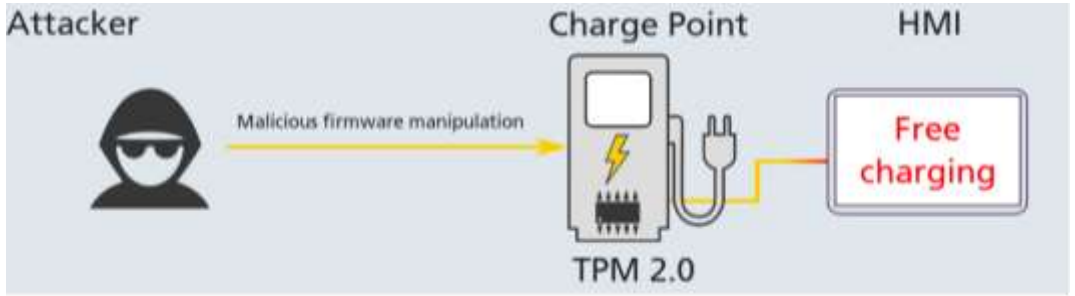
➔ A (large number) of compromised CPs, could attack the power grid or attack electric vehicles

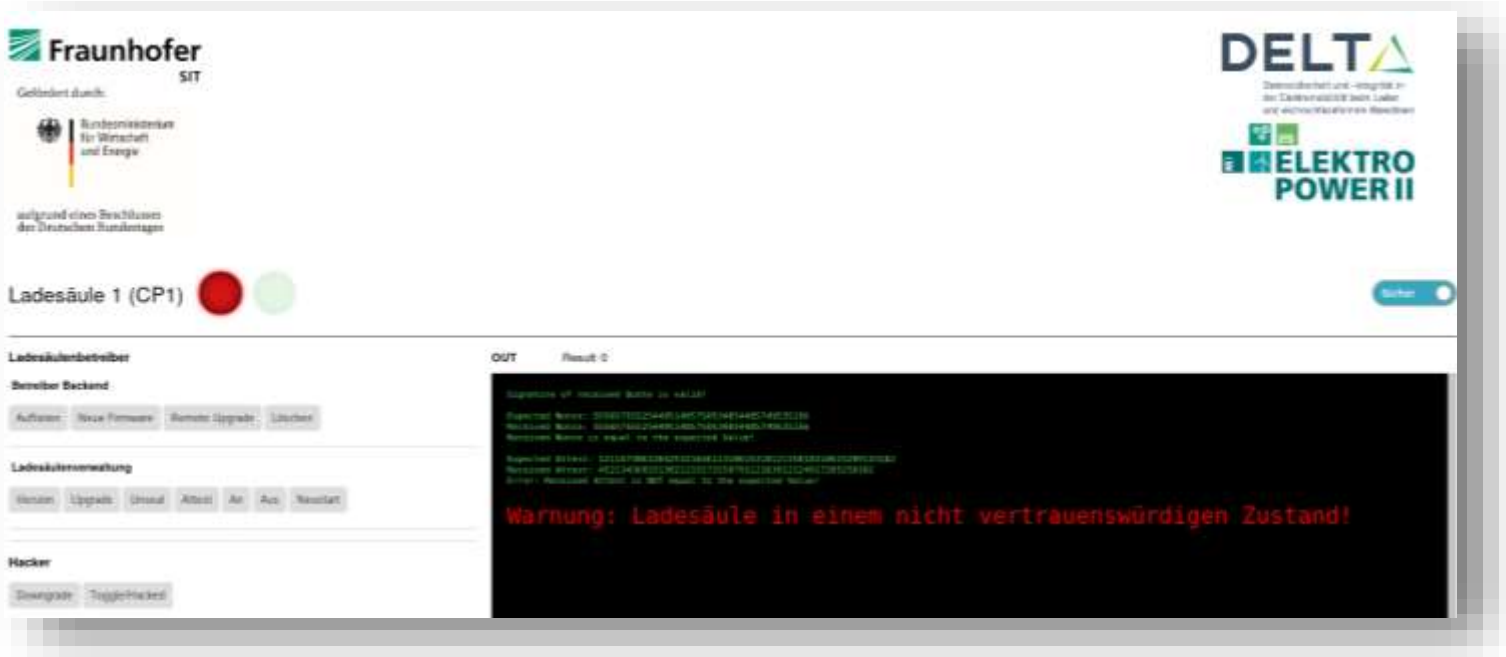
Attack on Keba P30 [Dal17]

[Dal17] M. Dalheimer. Ladeinfrastruktur für Elektroautos: Ausbau statt Sicherheit - Warum das Laden eines Elektroautos unsicher ist, 34C3, 2017

Securing Charge Points – Measured Boot and Remote Attestation

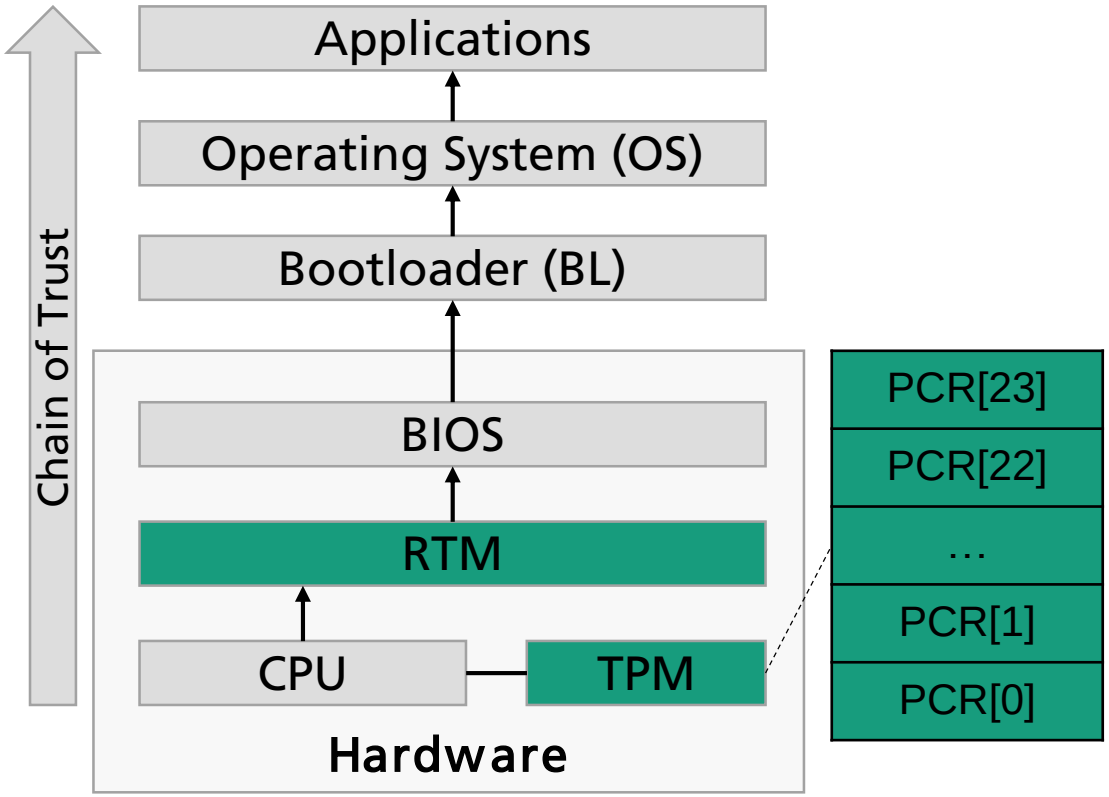
- Local verification of CP state too expensive and slow
  - Would require regularly sending a skilled technician to analyze all CPs
- Remote attestation to detect firmware manipulations using TPM-based measured boot



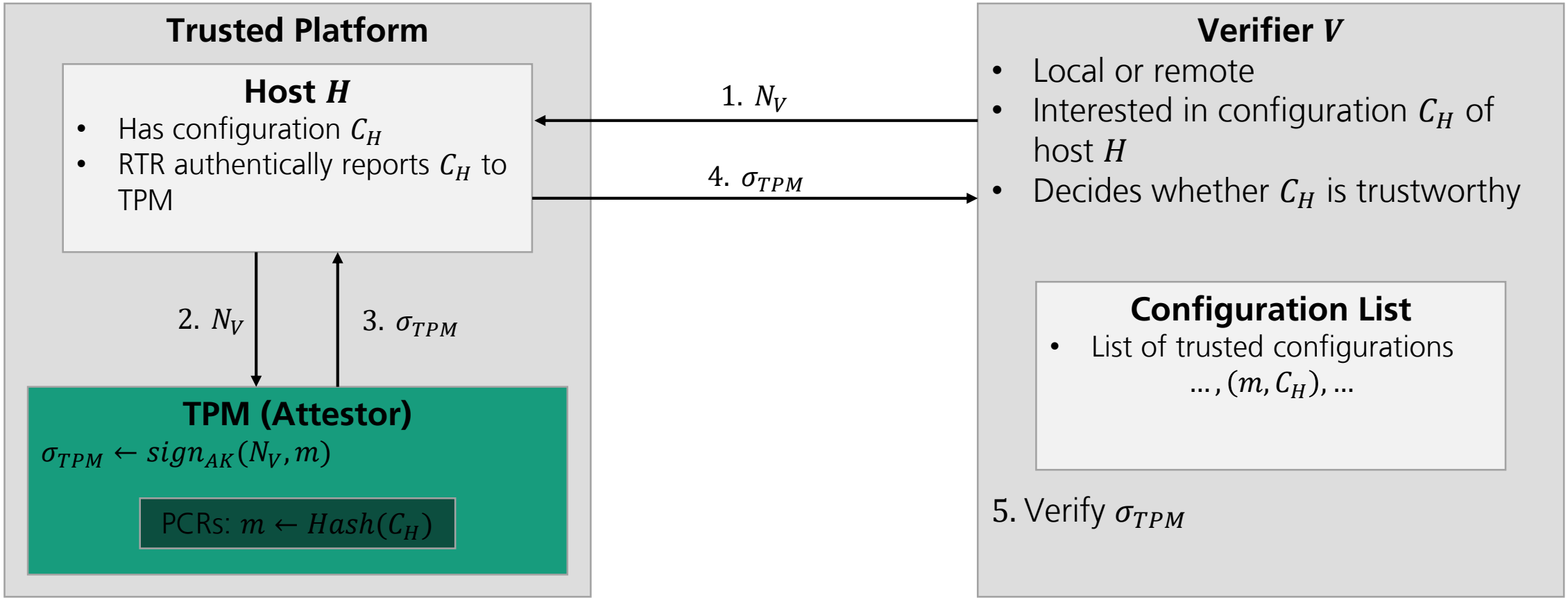


Securing Charge Points – Measured Boot using TPM

- Measurements of software states are stored in Platform Configuration Registers (PCRs)
  - PCRs usually initialized with 0
  - PCRs are extended with software states, i.e., $PCR[n]_{i+1} = Hash(PCR[n]_i || measurement)$
    - RTM measures BIOS
    - BIOS measures BL
    - BL measures OS
    - OS measures Applications
- PCRs for Authorization
  - PCRs must define a specific state to satisfy a policy
  - Use cases, e.g.,
    - Sealing hard disk encryption key
    - Sealing VPN keys
    - Attestation

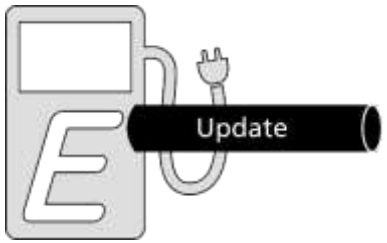


Securing Charge Points – Remote Attestation using TPM (simplified)

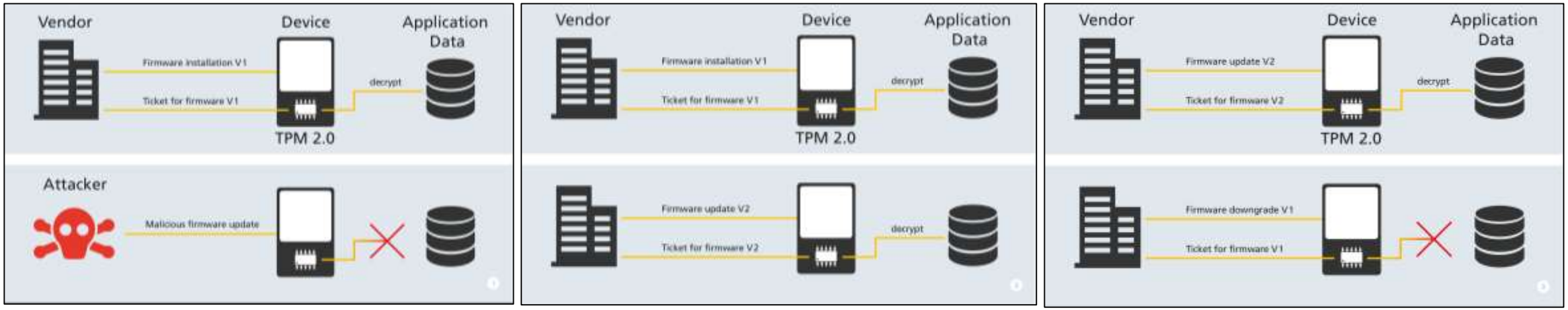


N_V: Nonce chosen by V
C_H: Current configuration of host H
σ_{TPM}: Signature over PCRs and Nonce using AK

Securing Charge Points using Trusted Computing – Secure Update



- Secure Over-the-air (OTA) update required for bug-fixes (functional, security), feature upgrades
- TPM 2.0 based Secure OTA Update Protocol
  - Authenticity, integrity, and confidentiality of update package
  - Downgrade protection, stop system if an older firmware has been installed
  - Allow only the original manufacturer to read / write firmware



[FKR16] A. Fuchs, C. Krauß , J. Repp. Advanced Remote Firmware Upgrades Using TPM 2.0, IFIP SEC, 2016

Attacks on Privacy

- Charging and billing process may lead to privacy problems
- Current (PnC) protocols do not consider privacy protection
  - ISO 15118 User / Contract ID can be read by all entities
  - Tag IDs of charging cards can be read by all entities
- Involved entities gain knowledge of a lot of personal data which is not required for their operation
- Identification of user and used charge points possible
  - Generation of movement or user profiles
  - Possibly deducing driving habits
- Current (PnC) protocols violate the European General Data Protection Regulation (GDPR)

	EV	CP/CPO	CCH	MO
CDR		✓	✓	✓
Charging Parameters	✓	✓		
Contract Certificate	✓	✓		✓
EMAID	✓	✓	✓	✓
EVCCID	✓	✓		
EVSEID	✓	✓	✓	✓
Location	✓	✓	✓	✓
MeterID	✓	✓	✓	✓
Power Consumption	✓	✓	✓	✓
Time	✓	✓	✓	✓

Example: Personal Data in PnC [ZSZK18]

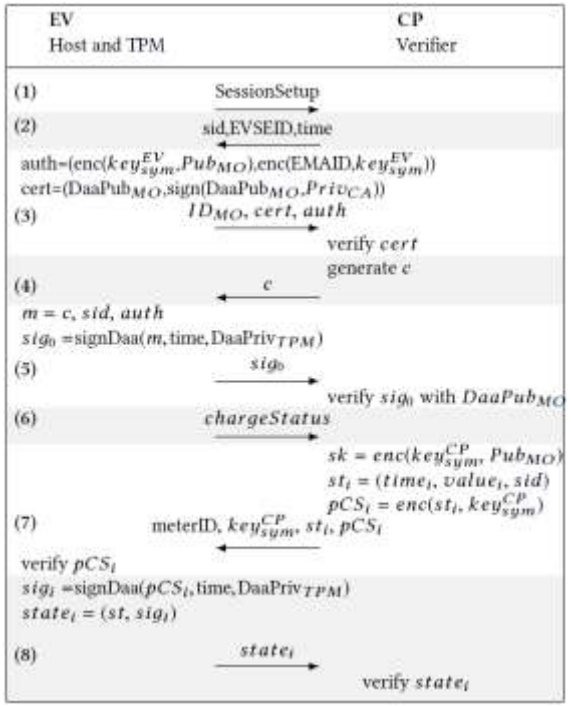
[ZSZK18] D. Zelle, M. Springer, M. Zhdanova and C. Krauß. Anonymous Charging and Billing of Electric Vehicles, ARES, 2018

Protecting Privacy

- Transparency Enhancing Technologies (TETs)
  - Inform user and get consent
  - Enable EV users to make informed and effective decisions on data protection relevant information sharing

TET developed within the SeDaFa project
(HMI design by IAD, TU Darmstadt)

- Privacy Enhancing Technologies (PETs)
  - Example: Privacy- preserving billing process using Direct Anonymous Attestation (DAA)



[ZSZK18] D. Zelle, M. Springer, M. Zhdanova and C. Krauß. Anonymous Charging and Billing of Electric Vehicles, ARES, 2018

Conclusion

- E-mobility will be an important part of our mobility
- Technologies, standards etc. still under development
- Many security and privacy challenges require additional research and development
- Ongoing research at Fraunhofer SIT
  - Development of draft protection profiles for CPs, EVs, and backend connection
  - Development of technical guidelines and prototypical implementations
  - Integration and evaluation of security solutions in test fields, e.g., charging infrastructure of the Fraunhofer LamA (Charging at Work) project

Fraunhofer SIT: Secure Charging Demonstrator

Contact

Prof. Dr. Christoph Krauß

Fraunhofer Institute for Secure Information Technology SIT
Head of Department Cyber-Physical Systems Security
Rheinstr. 75 | 64295 Darmstadt | Germany

christoph.krauss@sit.fraunhofer.de
www.sit.fraunhofer.de