GRACE HOPPER CELEBRATION

ANITA B.ORG

SP101: ACM Award Winning Research in Cybersecurity

#GHC19

Secure Free-floating Car Sharing for Offline Cars

Alexandra Dmitrienko
alexandra.dmitrienko@uni-wuerzburg.de

Whoami?

- **Professor at the University of Würzburg in Germany:** Leading the Secure Software Systems Research Group at the Chair of Software Engineering (since 2018)
- **10+ years in security research** in large security hubs in Europe: Ruhr-University Bochum (DE), Center for Advanced Security Research in Darmstadt (CASED), ETH Zurich (Switzerland)
- **Excellent Research:** ERCIM STM Award for the best Ph.D. Thesis on Security and Trust Management (2016), Doctoral Student Honor Award from Intel (2013)
- **Solving practical problems:** 5 years at Fraunhofer Institute for Secure Information Technology working in close collaboration with industry on practical problems

ACM Award winning research:

Published at ACM Conference on Data and Application Security and Privacy (2017)

Joint work with Christian Plappert (Fraunhofer SIT)

Granted an award for excellent innovation from Gesellschaft zur Förderung des Forschungstransfers (GFFT) in 2016

Why Car Sharing?

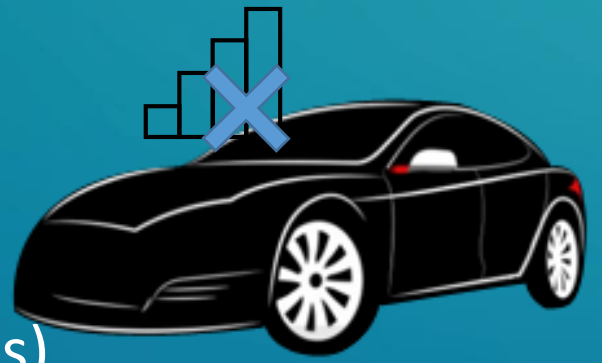
- More efficient use of cars
- Cost effective
- Reducing traffic
- Minimising air pollution

State-of-the-art Car Sharing Solutions

- Two usage models:
  - Station-based (return car from where taken)
  - Station-free (free-floating) – only in cities with network coverage, cars require online connection
- Types of car keys:
  - Smartcard, Smarphone app
- Limitations
  - Online cars in free-floating model
  - Intrusive car modifications
  - Unclear security guarantees (especially for app-based solutions)

Goals and Contributions

- Address current limitations in one solution
  - Offline cars (also for free floating model)
  - Compatibility to off-the-shelf cars
  - Enhanced security concept (also for app-based solutions)

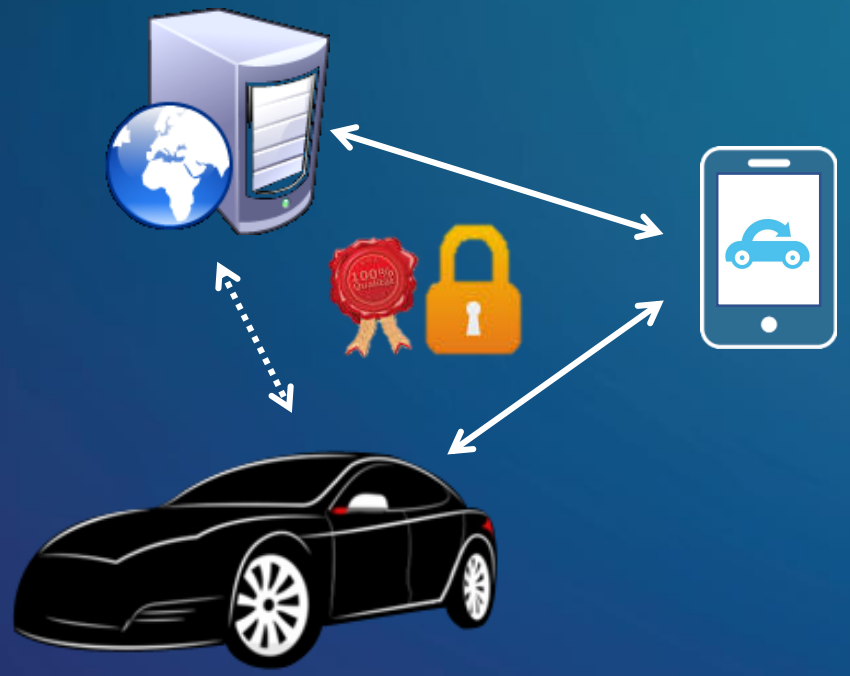


- Compatibility to existing RFID systems

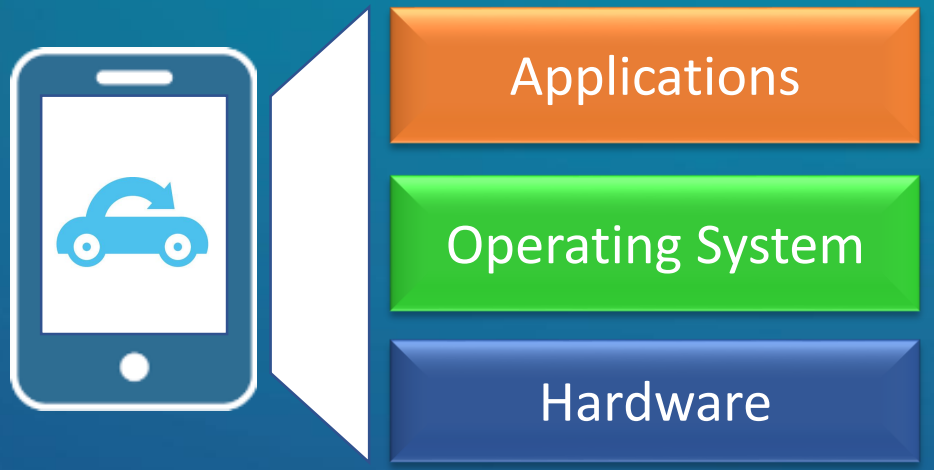
- Flexibility: Various deployment options to support heterogeneous client platforms

Enhanced Security

Secure Communication

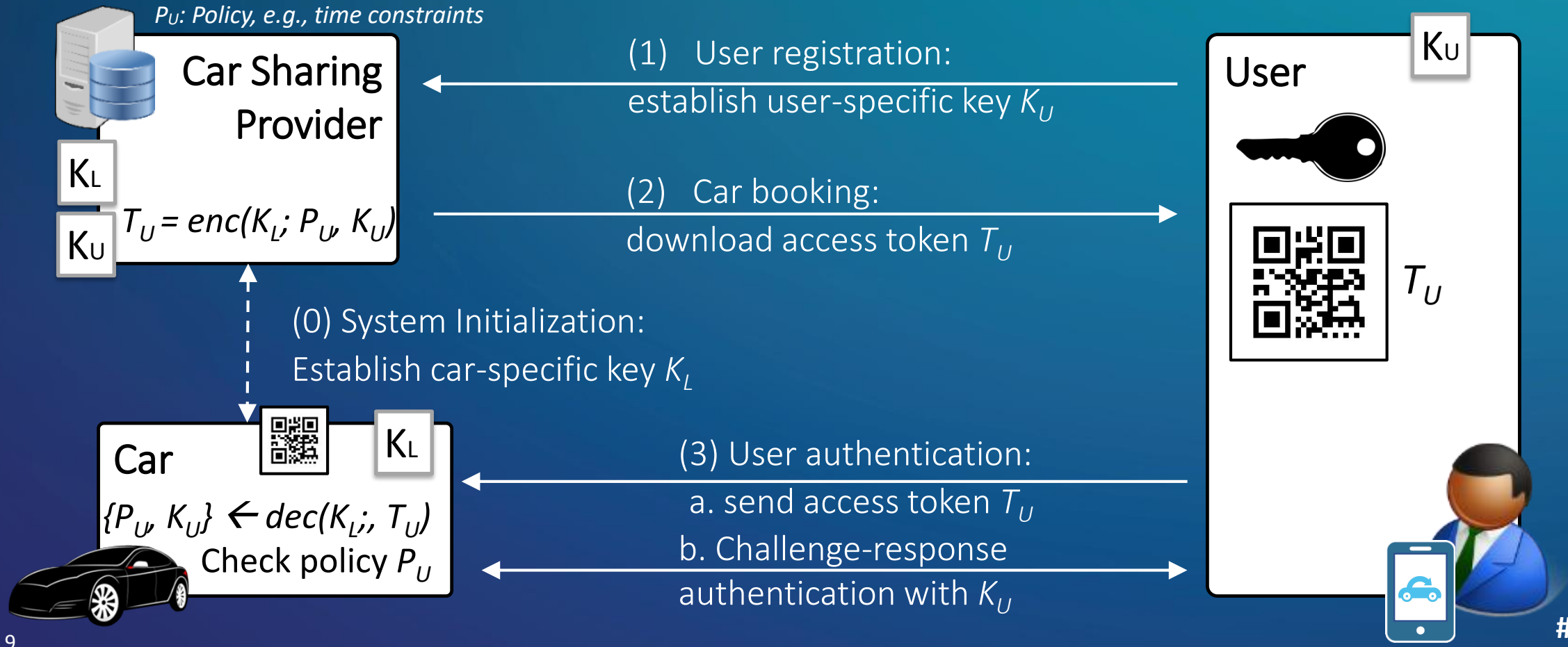


Platform Security



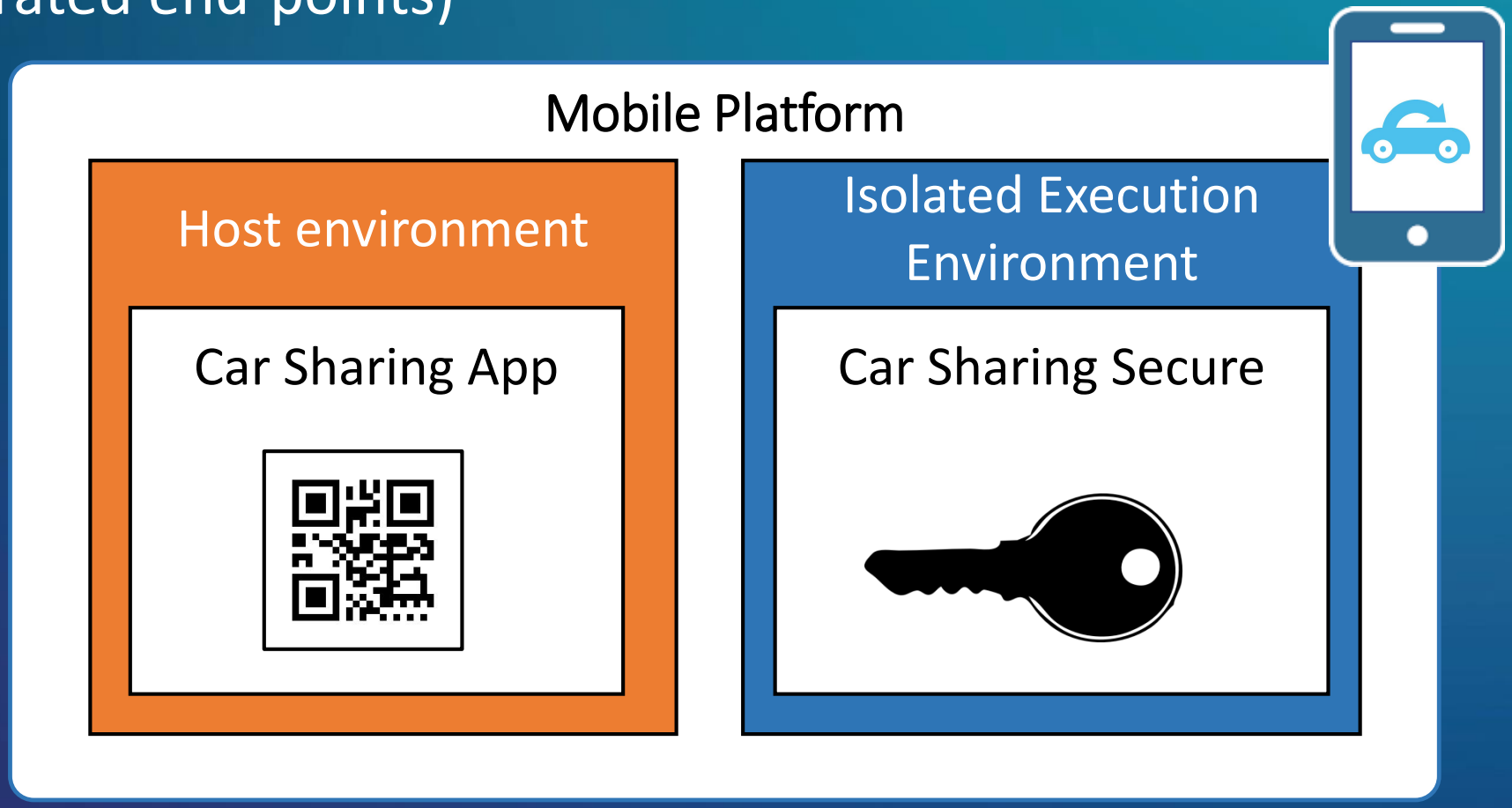
Two-Factor User Authentication (simplified)

- First factor: User-specific (AES 128 bit) key K_U
- Second factor: Access token T_U (with user access policy P_U)



Client-side Protection of Authentication Secrets

- Two authenticators are handled in isolated environments (two separated end-points)



Deployment Options

Host environment

Car2Share App

NFC

Smart card

Bluetooth

IPC

ASSD card

Runs DESFire EV1 applet

Smart Watch

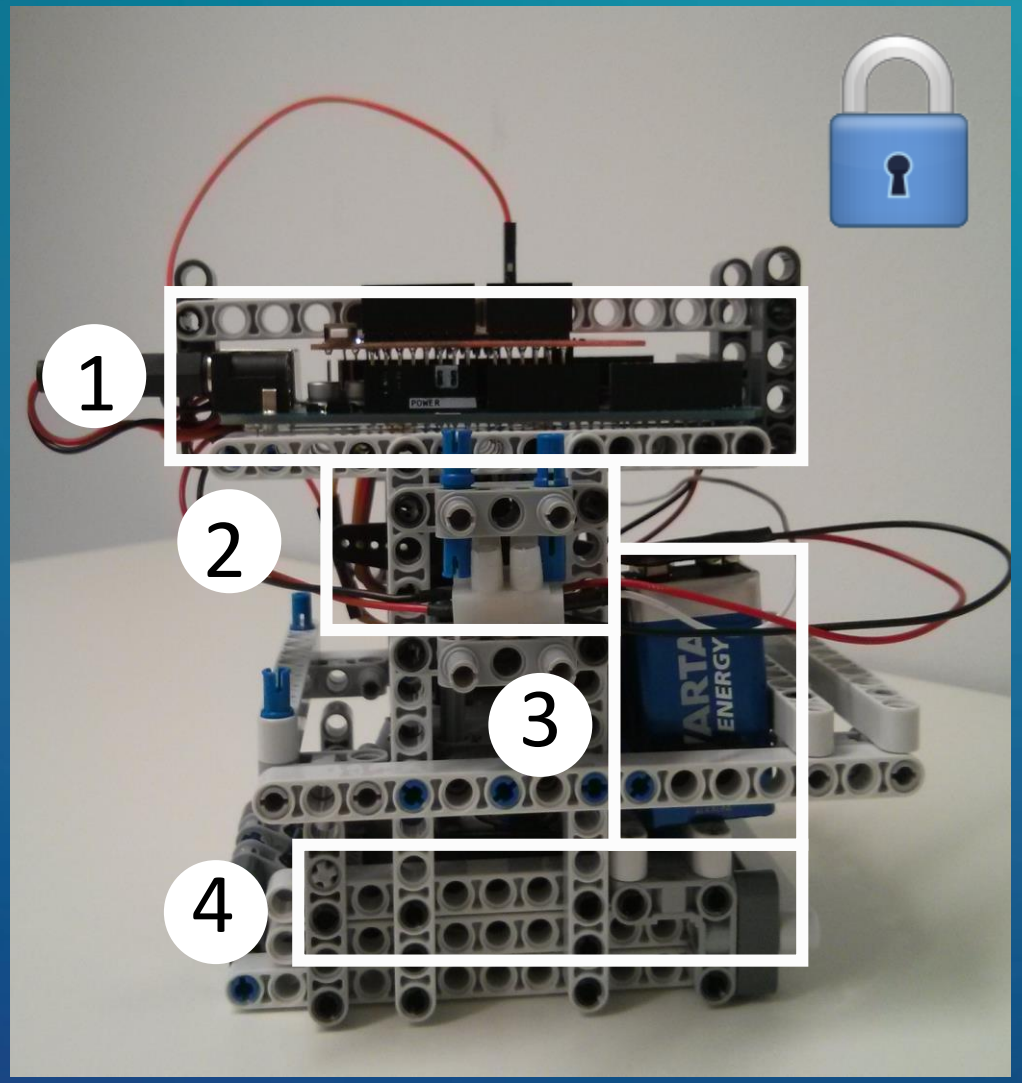
Runs jCardSim emulator
+ DESFire EV1 applet

Compatibility to Legacy Cars: Car Key Fob as a Proxy

- Car key fob is placed into the telematics box
- The box is placed into the car and communicates wirelessly with the phone
- Box has a mechanical ‘finger’ that pushes the buttons on the key fob to unlock the car

Demo Car Lock

- Based on Lego
  1. Arduino with BLE shield
  2. Servo motor
  3. Power supply
  4. Car key fob



Car Sharing Demo

Take away

Our car sharing solution provides:

- **FUNCTIONAL IMPROVEMENTS**: support for offline cars, also for free-floating usage models
- **STRONG SECURITY** thanks to 2-Factor authentication and processing both authentication factors in strong isolation
- **COMPATIBILITY** to legacy cars and to well-established standards (Mifare DesFire EV1)

Please remember to complete the session survey in the mobile app.

THANK YOU

YOU CAN *FOLLOW ME* @

linkedin.com/in/sdmitrienko

GRACE HOPPER CELEBRATION

ANITAB.ORG

#GHC19