**Smart Keys for Cyber-Cars: Secure Smartphone-based NFC-enabled Car Immobilizer**

**Christoph Busold¹, Alexandra Dmitrienko², Ahmad-Reza Sadeghi¹, Hervé Seudié³, Majid Sobhani³, Ahmed Taha³, Christian Wachsmann¹**

¹ Intel CRI-SC, TU Darmstadt, Germany ² Fraunhofer SIT, Darmstadt, Germany ³ TU Darmstadt, Germany

---

### Motivation
- Increasing integration of smartphones into modern automotive systems
- Customized access without physical key transponder possible: e.g., delegation of rights, location-based access
- Security of current available automotive smartphone-based solutions unclear since undisclosed from review

### Requirements & Challenges
- Fast authentication for positive user experience
- Remote key management (issuing/revocation)
- Direct delegation of access rights (without the issuer)
- Context-aware access policies (e.g., time-limited)

---

### General Architecture
- Token-based authentication system
- Enables secure deployment and storage of tokens
- Supports token delegation and revocation

---

### Design
- **Platform Security Architecture**
  - Secure storage to protect sensitive data (e.g., crypto keys)
  - Isolated execution to protect sensitive code
  - Access control to security sensitive code and data

---

### Secure Protocols
- Use well-established crypto primitives (AES, SHA-1, RSA)
- Formal tool-aided protocol verification (ProVerif)

---

### Related Work
- Prototypes of Smartphone-based immobilizers available but their security is unclear since undisclosed
- Existing open specifications of security stacks are focusing exclusively on immobilizer part
- No automotive solution proposes delegation of access rights

---

### Implementation
- **Platform**
  - NFC-enabled Galaxy S3 smartphone
  - Arduino board as proof-of-concept immobilizer platform
  - Secure microSD card as trusted execution environment

---

### Performance
- Performance-critical parts use symmetric crypto
- Tokens optimized for small NFC bandwidth
- Authentication protocol runs in under 700 ms

---

**Contacts:**
- christoph.busold@trust.cased.de
- alexandra.dmitrienko@trust.cased.de
- herve.seudie@trust.cased.de