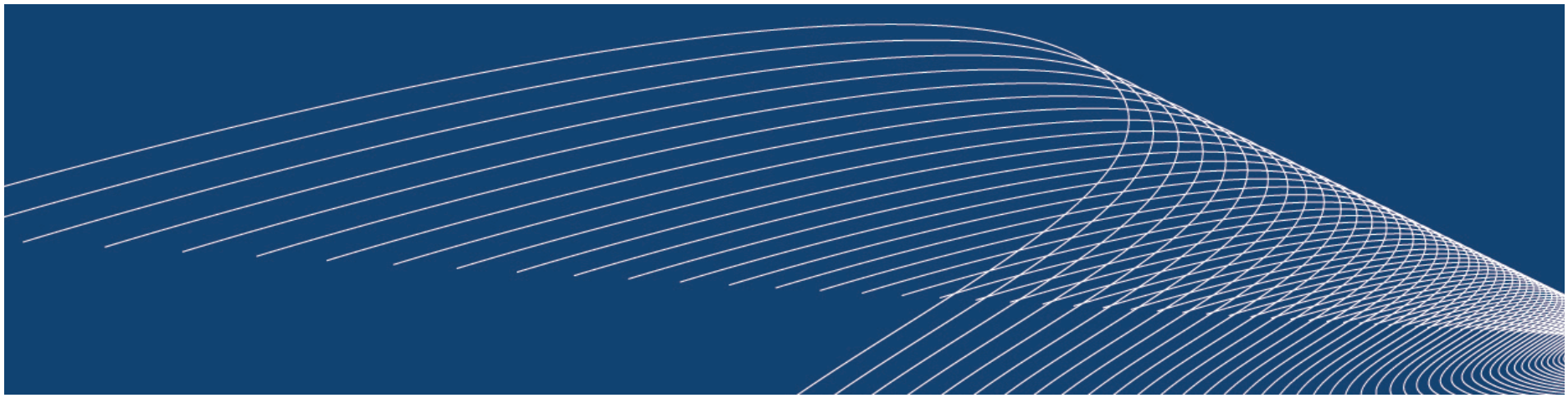
VOLKSWAGEN

AKTIENGESELLSCHAFT



Security Requirements of C2C Applications

Amer Aijaz

Electronic Research, Volkswagen Group

19.11.2006

CAR 2 CAR

COMMUNICATION CONSORTIUM

C2C Scenario

Application: Safety warnings

- Vehicle – Vehicle
- Infrastructure – Vehicle

Communication technology: DSRC

- Single hop
- Multiple hop

Security Threats

- Masquarading
- Manipulation
- Replay attacks
- Privacy violations
- Criminal misuse & Repudiation

Security Objectives

- Identity Authentication (vs. Masquarading)
- Integrity Verification (vs. Manipulation)
- Freshness Checks (vs. Replay Attacks)
- Anonymity (vs. Privacy violations)
- Privacy Revocation (vs. Criminal misuse)
- Legal proof of misuse (vs. Repudiation)

1. Identity Authentication

Proof of :

- being a C2CC validated sender
- being within validity constraints
- not being a black-listed node

C2CC challenges:

- Very quick authentication
  - ↳ << Human reaction delay = 1 sec
- Offline authentication issues
- Black listing nodes

2. Integrity Verification

Proof that message is:

- originated by claimed originator
- unaltered by any Man-in-the-Middle

C2CC challenges:

- Message processing glut due to:
  - ↳ heavy traffic situations
  - ↳ jamming, DoS attacks

3. Freshness Checks

Reject messages failing:

- Time freshness
- Position freshness
- Other situation relevance tests

C2CC Challenges:

- Using local status to judge remote situation
- Manipulation of reference information

4. Anonymity

No person relatable to:

- Message (content, encoding, encryption)
- Sender of Message (address, credentials)

C2CC Challenges:

- Anonymizing the PKI

5. Privacy Revocation

Required to:

- discourage criminal misuse
- collect evidence against criminal misuse

Isolate driver / vehicle

- Directly: Deny enterance in closed system
- Indirectly: Destroy reputation

C2CC Challenges

- Quick isolation

6. Legal Proof of Crime

Required to:

- Technically support legal enforcement
- Punish criminals

C2CC Challenges:

- Differentiating between:
  - System fault
  - Unintended mistake
  - Criminal intention