1st C2C-CC Public Workshop on Security

Welcome and Agenda Setting

Berlin, November 16, 2006

H.-J. Vögel, Chair Working Group Security&Middleware

CAR 2 CAR
COMMUNICATION CONSORTIUM

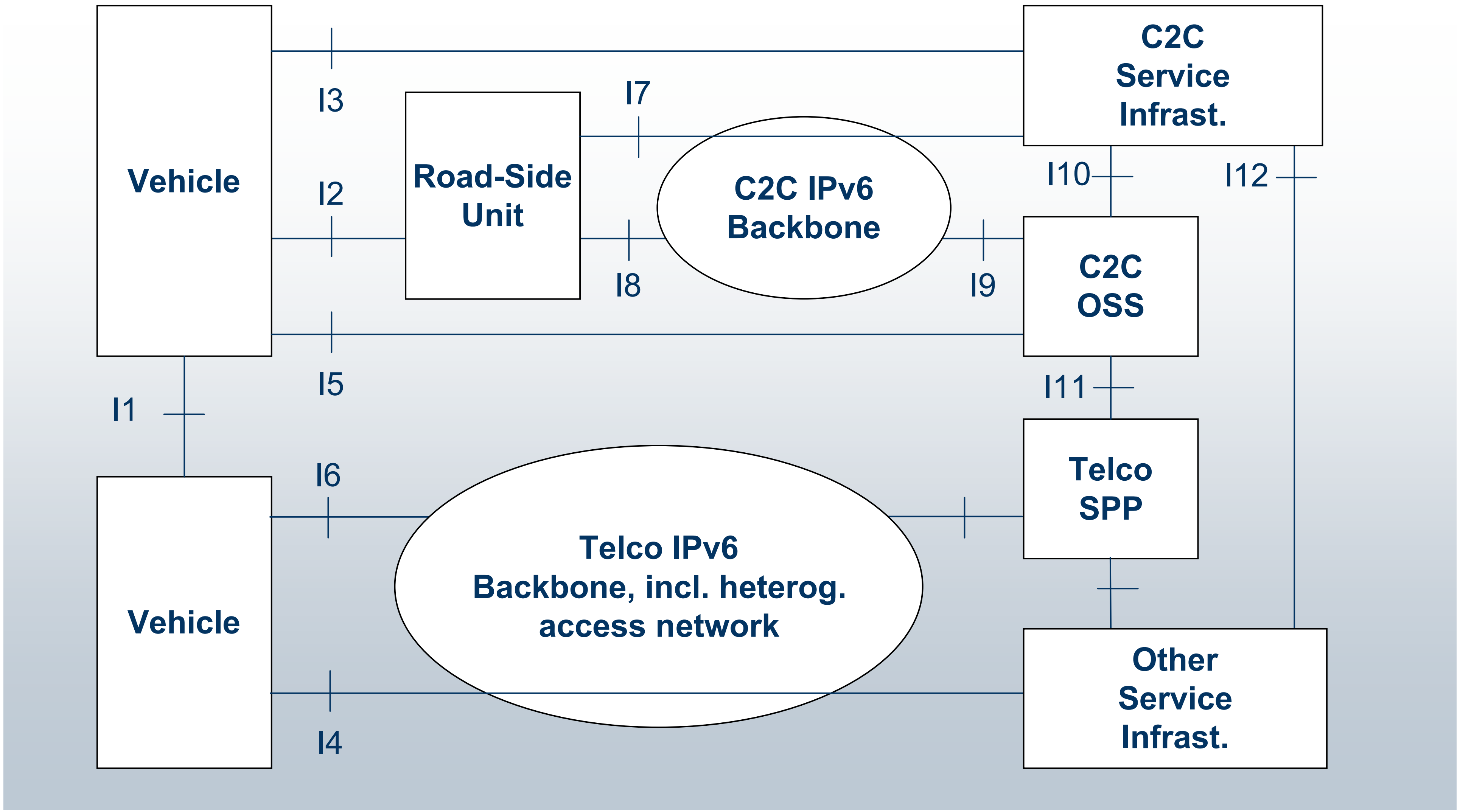
Goals of this workshop

- Synchronize research community with current state of C2C-CC requirements discussion
- Collect overview of solution proposals from research side
- Create baseline for public discussion on security requirements for C2C-CC systems
- Agree on public whitepaper for C2C-CC security

C2C-CC Security Principles

- C2C-CC comprises vehicle-vehicle and vehicle-infrastructure communication
- C2C and C2I message exchange in “ad-hoc” fashion
- Infrastructure-based identity management, certificate renewal and revocation
- Focus on system and functional integrity, less content confidentiality
- Privacy among top concerns, but not at any cost
- Balance technical security vs. plausibility & reliability

Reference Model



System Integrity

- Trust in message content
- Protect against malicious false information injection
- Ensure graceful system response to faulty information
- Requires balanced combination of technical security and system dependability measures
- Provide means to isolate malicious and faulty vehicles rapidly
- What are the conditions for certificate revocation?
- Performance:
  - Real-time requirements with periodicity from 10s to sub 100ms
  - Scalability to several hundred nodes within visibility range

Confidentiality

- Usually not: C2C-CC information shall be openly shared to improve traffic efficiency and road safety
- Messages need to be authentic, but their contents needn't be encrypted
- Potential exception: where closed group communication can be more efficiently addressed through temporary peer authentication and subsequent secure session
- But: this is dependent on business models
    - Infrastructure deployment may ride on business models requiring exclusive access to information – how can this be protected?
    - Proprietary use cases co-existing with standardized use cases not ruled out (yet?)

Privacy

- Protect against typical privacy-infringing profiling
- No fixed addresses per vehicle
- No permanent unique certificate per vehicle
- Ensure system maintainability
  - Allow faulty vehicles to be identified
- Constraints:
  - Trajectory backtracking, e.g. by plausibility verification and inference from recorded message stream might still be possible
  - Can this be countered for selected applications in areas and/or situations where recording is likely?

Non-technical areas of activity

Security discussion is influenced by

- Legislation and regulation
  - Law enforcement
  - Privacy requirements
  - Licensing and certification requirements
- Certification
  - Scope? Authority? Periodicity?
- Socio-economic
  - Business models and business objects requiring protective measures
  - Overall trustworthiness and acceptance of the system
  - Insurance and liability aspects

Standardization

- IEEE WAVE 1609
- IEEE 802.11