Secure Vehicle Communication

Discussion on Identity Management

Panos Papadimitratos

EPFL

System view

SEVECOM

- Vehicular communications system participants
  - Users
  - Network nodes
  - Authorities
- Users: individuals that operate vehicles
  - Focus on network operation and device communication

System view (cont'd)

SEVECOM

- Network nodes
  - *Infrastructure*
    - Roadside units
      - Static, quasi-static
    - Mobile infrastructure
      - Public safety vehicles
        - **Police, road assistance, firefighters, ambulances**
      - Buses
  - *Non-infrastructure vehicles*
- Servers at the wire-line part of the network

“Physical” world identity

SEVECOM

- Drivers and vehicles already identified in multiple ways
  - Drivers
    - Name
    - License number, mailing address, date of birth
    - ...
  - Vehicles
    - Vehicle identification number
    - Registration number
    - Type of the vehicle
    - …

Question 1

SEVECOM

- What is the relation between the “physical” and the “VeCom” world identities?
  - Integration
  - Extension
  - Tranquility/preservation
    - Basic design principle or *de facto* requirement?

“VeCom” identity

SEVECOM

- “Physical world” set of identity attributes
- Network identifiers
  - At different layers of the protocol stack
- Service identifiers/credentials
- Cryptographic keys and credentials

Question 2

SEVECOM

- What are the required system properties?
  - Liability
    - Accountability
  - Privacy
  - Contradictory requirements and objectives
- How well are these requirements understood and defined in the context of vehicular communication systems?

Privacy

SEVECOM

- Information hiding - Privacy
  - VeCom system operation does not disclose or allow inferences on the personal and private information of the users
- What distinguishes VeCom when it comes to transactional communication?
  - E.g., service access
  - Privacy ? confidentiality

Privacy (cont'd)

SEVECOM

- Is *anonymity* a requirement in the vehicular networking context?
- Actions (e.g., messages) of nodes remain *anonymous* with respect to a set of observers
  - In other words, the identity of the node taking an action remains hidden from the observers

Privacy (cont'd)

SEVECOM

- At minimum: observer unable to learn if an action is taken by node *A*, but:
- Observer may be able to *guess* that node *A is more likely* to have acted than node *B*
- Stronger notion of anonymity?

Impact on the system design

SEVECOM

- Hypothesis
  - *Infrastructure nodes: No anonymity*; instead, rich description of identity and attributes
  - *Non-infrastructure nodes: Anonymity*
- Facts
  - Managed identities
  - Security services (e.g., access control, entity and data authentication)
  - Liability

Impact on the system design (cont'd)

SEVECOM

- Example: Instantiation of authorities
  - New operational assumptions
    - Fine-grained location-dependent deployment and operation
    - Delegation
  - Interaction with nodes
    - Registration, node bootstrapping
    - Renewal and revocation of credentials
  - Separation of privilege
    - Issuance of anonymous credentials
    - Linking of traffic/data to vehicle

Conclusions

SEVECOM

- Definition of basic assumptions and requirements
- Incremental integration of (functionality for) additional requirements, as agreed upon and as on-board computers can support them
- Identity management assumptions and requirements can strongly influence the architecture of evolving vehicular communication systems