A Privacy Aware and Efficient Security Infrastructure for Vehicular Ad Hoc Networks

Klaus Plößl
Hannes Federrath
University of Regensburg

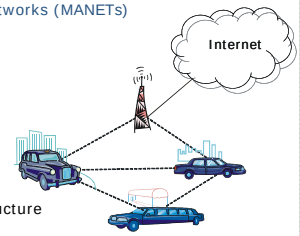
Workshop on Security in Information Systems 2007
12.06.2007

Outline

- Introduction
- Security Requirements
- Proposal
  - Initialization
  - Asymmetric Part
  - Symmetric Part
- Evaluation
- Conclusion and Further Aspects

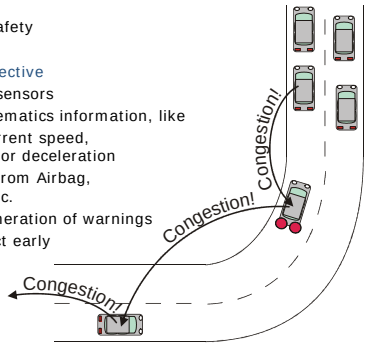
Vehicular Ad Hoc Networks (VANETs)

- Subgroup of Mobile Ad Hoc Networks (MANETs)
- Main difference
  - Router = Vehicle
- Particularities
  - High speed
  - High scalability needed
  - Restricted node movement
  - Assistance of fixed infrastructure is feasible
- Includes
  - Vehicle-to-vehicle communications (V2V)
  - Vehicle-to-roadside communications (V2R)



Vehicular Ad Hoc Networks (VANETs)

- Main objective
  - Increase road safety
- Achievement of objective
  - Vehicles act as sensors
  - Exchange of telematics information, like
    - Location, current speed, acceleration or deceleration
    - Sensordata from Airbag, ABS, ESP, etc.
  - If necessary generation of warnings
  - Drivers can react early



Application Categories

- Warnings and telematics information (W)
  - E.g.: full brake application warning, congestion warning, airbag activation warning, beacons, ...
  - Geocast
- Alarm signals and instructions (A)
  - E.g.: signals from police cars or fire engines, speed limits, intersection assistance, ...
  - Geocast and unicast
- Value-added services (V)
  - Mostly not critical for traffic safety
  - E.g.: Internet on the road, location based services, remote car maintenance, ...
  - Mainly unicast

Terms and Assumptions

- Security Infrastructure
  - Facilitates mutual trust
  - Enables cryptography
  - Includes all technical and organizational measures and facilities needed to fulfill the protection goals
- Assumptions
  - In-car sensor data is correct
  - Integration of correct time and position information in all messages
  - Correct time and position information is available from other infrastructure like Galileo

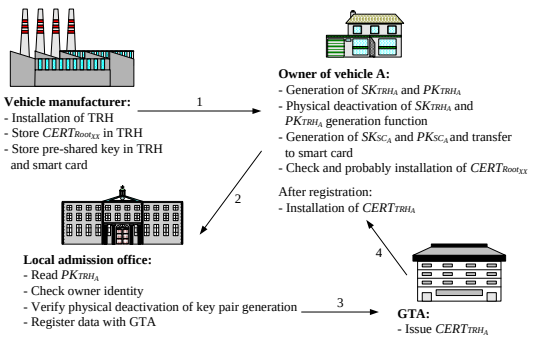
Security Requirements

		W	A	V
I1	Data integrity	x	x	x
I2a	Immediate sender authentication		x	
I2b	Ex post accountability	x		x
P1	Protection against profile generation	x	x	x
P2	Protection against surveillance	x	x	x
C1	Different levels of confidentiality	x	x	x
C2	Protection of the security infrastructure	x	x	x
A1	Computational and bandwidth efficiency	x	x	x

Proposal: Overview

- Asymmetric part with PKI
  - Vehicle-related identity
  - Special privileges by short-term certificates
  - Integrity protection of road safety messages (A and parts of W)
  - Basic authentication
  - Protection of key management messages for the symmetric part
- Symmetric Part
  - Integrity protection (V and parts of W)
  - Encryption
  - Changing pseudonyms
  - Needs tamper-resistant hardware
  - Employs geographically distributed trusted third parties (GTTPs)

Proposal: Once-Only Initialization



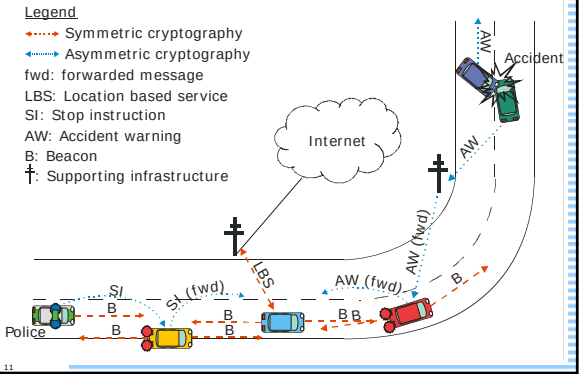
Proposal: Asymmetric Part

- Message format asymmetric part

Data with address information	Digital Signature	$CERT_{Sender}$

- Usable after the once-only initialization
- Used for
  - Road safety related messages
  - Alarm signals
  - Instructions
- Revocation checks
  - Not critical for warnings
  - Not necessary for alarm signals and instructions
    - Short-term certificates with attributes

Proposal: Example



Proposal: Symmetric Part

- Used for
  - Beacons
  - Messages of the value-added services
- Requires communication with GTTP from time to time
  - Distribution of symmetric keys for
    - Message encryption
    - Message authentication
  - Distribution of pseudonyms
    - GTTP has to be independent from law enforcement
    - Only GTTP knows relationship between pseudonyms and VRI
- Better performance than asymmetric part
- Exclusion of malicious nodes possible

Proposal: Symmetric Part

- Message format symmetric part

Data with address information	PA	MAC_1 with $k_{MAC_{PA}}$	MAC_2 with $k_{MAC_{ALL}}$

ciphered with k_c

- k_c and $k_{MAC_{ALL}}$
  - Identical for all users in the same area
  - Changed periodically
- PA and $k_{MAC_{PA}}$
  - At least one for each node
  - Changed periodically
- Message processing and key storage in TRH
- For value-added services application specific encryption possible

Evaluation

- Data integrity (I1)
  - Digital signature
  - MAC_2
- Immediate sender authentication (I2a)
  - Short time certificates
- Ex post accountability (I2b)
  - Digital signature based on VRI
  - MAC_1
- Protection against profile generation (P1)
  - Changing pseudonyms

Evaluation

- Protection against surveillance (P2)
  - Independent GTTPs
- Different levels of confidentiality (C1)
  - Possible by means of VRI certificates, symmetric keys or other service specific key material
- Protection of security infrastructure (C2)
  - Encryption of key management messages
  - Usage of TRH

Evaluation

- Computational and bandwidth efficiency (A1)
  - Assumptions
    - Message length: approximately 300 byte
    - RSA with SHA-256 (key length 2048 bit)
    - HMAC SHA-256 (key length 192 Bit)
    - AES (key length 192 Bit)
    - Pseudonym 48 Bit
  - Asymmetric part
    - Digital signature + certificate
    - 2048 bit + (2048 bit + 2048 bit) = 768 byte
    - Total 1068 byte

      ⇒ 72% Security overhead

Evaluation

- Computational and bandwidth efficiency (A1)
  - Symmetric Part
    - PA + 2 * HMAC
    - 48 bit + 2 * 256 bit = 70 byte
    - Total 370 byte

      ⇒ 19% Security overhead
  - No certificate revocation list necessary
  - Overhead for key management negligible
  - Far the most messages use symmetric part
    - Much more efficient than asymmetric protection
  - Computational delay
    - 100ms (asymmetric part)
    - 0,165 ms (symmetric part)

Conclusion and Further Aspects

- Conclusion
  - All requirements are fulfilled
  - Protects privacy of participants
  - Is very efficient
- Further aspects
  - Refine proposal
    - Schedule for changing the symmetric keys and pseudonyms
    - Best size of the geographic regions for the GTTPs
  - Specify when GTTP has to reveal connection between a given pseudonym and VRI
- Contact:
  - Klaus.Ploessl@wiwi.uni-regensburg.de