Security of vehicular communications

- vehicular safety communications
- design constraints
- attacker classes
- desired security services
- a security architecture

Vehicular communication (VC) systems

- motivations:

- VC promises safer and more efficient driving via ensuring that the right information is available at the right time at the right place
  - road condition warning, curve speed assistance, electronic brake light, collision warning, emergency vehicle signal preemption, …
- however, this will become reality only if VC cannot be misused to create accidents and to invade the privacy of the drivers

Vehicle communications activities

- projects
  - CVIS: Cooperative Vehicle-Infrastructure Systems
  - Coopers: Cooperative Systems for Intelligent Road Safety
  - Safespot: Cooperative Vehicles and Road Infrastructure for Road Safety
  - NoW: Network on Wheels
  - SeVeCom: Secure Vehicle Communications (CrySyS is partner)
- standardization
  - IEEE 802.11p: Wireless Access in the Vehicular Environment (WAVE)
  - C2C-CC: Car to Car Communications Consortium (Audi, BMW, Daimler, Fiat, Honda, Opel, Renault, Volkswagen, Volvo)
- legislation

  August 2008: "As part of its overall fight against road accidents and traffic jams, the Commission decided to reserve, across Europe, part of the radio spectrum for smart vehicle communications systems (so called co-operative systems). They are based on wireless communication technology and allow cars to 'talk' to other cars and to the road infrastructure providers. "

The SeVeCom Project

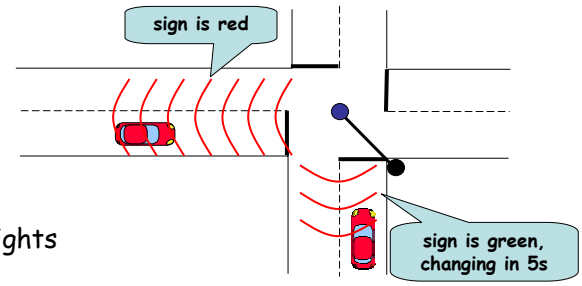
- Secure Vehicle Communications
- funded by the EC within FP6 (project no. 027795)
- started in Jan 2006, duration 3 years
- objectives:
  - secure communications specific to road traffic (safety messages)
  - development of a security architecture for vehicular communication systems (key and identity management, secure communication protocols, privacy, in-vehicle intrusion detection)
  - definition of a deployment road-map
- status:
  - baseline security architecture defined
  - HW platform identified
  - implementation and integration is in progress
  - extensive liaison with other related projects: C2C-CC, CVIS, SAFESPOT, COMeSafety, ..
- partners:
  - industry: Trialog, Daimler, CR Fiat, Bosch
  - academia: EPFL, U Ulm, KU Leuven, TU Budapest (BME/CrySyS)
- more information: ***www.sevecom.org***

Vehicular safety communications

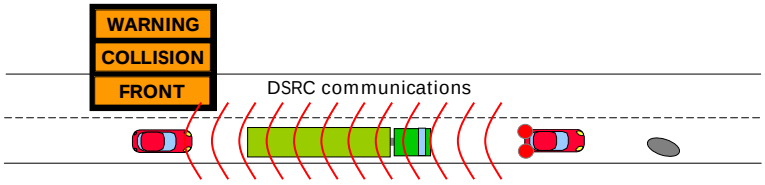
- a VSC system will allow vehicles to communicate with each other and with infrastructure elements
- network elements
  - road side units (RSU): network nodes embedded in road side infrastructure (e.g., traffic lights, road signs)
  - on-board units (OBU): network nodes embedded in vehicles
- both types of network nodes will consist of
  - general purpose processor and associated memory
  - a radio transmitter and receiver
  - interfaces to sensors as required
  - a GPS receiver (for non-stationary units)

Example applications of VSC

- curve speed warning
- traffic signal violation warning



- extended break lights



Attacker capabilities

- class 1: attacker with a programmable radio transceiver
  - can transmit and receive messages
  - replay or tunneling
  - denial of service (e.g., jamming)
  - RF fingerprinting
- class 2: attacker with access to an unmodified VSC unit
  - change location (of an RSU)
  - manipulate sensor readings
  - GPS spoofing
    - convince GPS receiver that it is at an arbitrary position

Attacker capabilities

- class 3: attacker with access to a modified VSC unit (compromised keying material)
  - cloning
  - modify behavior (e.g., override implausibility checks)
  - discover and exploit programming errors in other VSC units
- class 4: attackers with access to records and equipment operated by the vehicle manufacturer or the VSC unit manufacturer (insiders)
  - access to customer records
  - access to key generating data or escrowed keying material
  - RF fingerprinting database

Desired security services

- general requirement
  - the receiver of a VSC message should obtain an accurate picture of the state of the world, as far as the transmitter knew it
- specific security services
  - message integrity and origin authentication
    - to protect against spoofing and modification attacks
  - correctness of message content
    - needs some level of tamper resistance (at least FIPS 140 level 2 or 3; level 4 would be too expensive)
  - privacy
    - tracking users should not be made easier by the VSC system
    - requirements are different for public safety OBUs and RSUs
  - robustness
    - we must assume that some units will be compromised

    → how to cope with compromised units?
    - denial of service

A first attempt for securing VSC

- let's assume that there is a globally shared symmetric key in each unit
- features
  - message integrity and origin authentication can be based on a symmetric key MAC computation
    - only group membership is authenticated
    - RSUs and public safety OBUs cannot be differentiated from regular OBUs
  - perfect privacy
    - no one really knows who sent a message
  - no robustness
    - entire system can be compromised by breaking a single unit
  - no correctness
    - compromised units can send false information
    - compromised units cannot be reliably identified and revoked

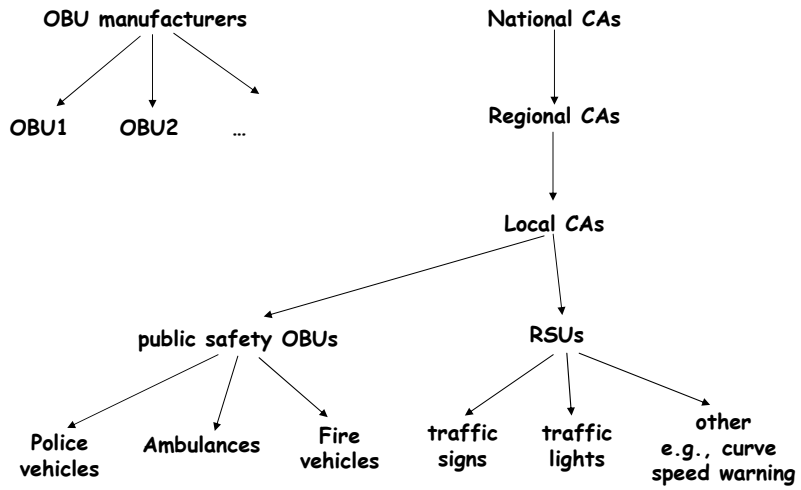
A better security architecture

- system should be based on public key cryptography
- general message structure:

  [header | payload | timestamp | position | key ID | signature]

  where key ID is a certificate or a key index
- design questions
  - What PKI structure to use?
  - Which signature algorithm to use?
- privacy requirements
  - regular OBUs need privacy protection
  - RSUs and public safety OBUs do not need privacy protection

Dual authentication structure



RSUs and public safety OBUs

- no need for privacy → straightforward PKI-style solution
- PKI structure
  - hierarchical
    - mirrors the naming and administrative hierarchy
    - imposes burden on the OBU (signatures should be verified for all certificates in the certificate chains and on related CRLs)
    - deployment requires each of the superior organizations to be operational prior to a subordinate entity
  - flat
    - single CA, but administrative hierarchy is kept
    - needs RAs for convenience
    - reduces the signature verification burden on OBUs
    - size of single CRL may be too long (but there exists optimization techniques such as partitioned, indirect, and delta CRLs)
    - deployment requires a national CA to be operational
    - the national CA must be highly available

RSUs and public safety OBUs

- certificate structure
  - X509 certificates are too large
  - VSC certificates should be optimized and contain only
    - the public key of the certificate holder
    - the scope of the certificate (geographic or functional)
    - the validity window of the certificate (expiry time)
    - a signature over the certificate
  - no identity string in the certificate, all relevant authorization information is in the scope field
- processing
  - standard signature generation / verification
  - scope verification
  - OBUs are expected to cache verified certificates, thus reducing the burden of re-verification for new certificates
  - certificate pre-loading (e.g., at the border of geographic regions)
  - CRL distribution

RSUs and public safety OBUs

- choice of algorithms
  - options
    - RSA (1024)
      - signature size: 128 bytes
      - public key size: ~128 bytes
      - signing time: 17 ms
      - verification time: 0.11 ms (with e = 3)
    - DSA (1024)
      - signature size: 40 bytes
      - public key size: 128 bytes
      - signing time: 8.8 ms
      - verification time: 10.75 ms
    - ECDSA (80)
      - signature size: 40 byte
      - public key size: 20 byte
      - signing time: ~ DSA signing time
      - verification time: ~ DSA verification time

    (tests carried out on 450MHz Pentium III)

Regular OBUs

- privacy protection is a requirement
  - anonymity – it is not possible to determine a vehicle's identity from its transmissions
  - unlinkability – it is not possible to determine that multiple transmissions were from the same source
- approaches
  - anonymous certificates
  - anonymous self-enforcing certificates
  - (static combinatoric schemes)
  - (dynamic combinatoric schemes)
  - group signatures

Anonymous certificates – a naïve solution

- each OBU has its own key pair certified using a PKI
- anonymous certificates
  - public key
  - validity period
  - identity of the signer
  - signature
- doesn't protect privacy
  - each message contains the certificate of the signer
  - messages signed by the same OBU can be linked through the fix public key

Anonymous certificates – a better solution

- issue a set of anonymous certificates to each OBU
- OBUs would change their active certificate periodically (e.g., every hour)
- CA needs to maintain a list of which certificate has been issued to which OBU (for revocation and law enforcement purposes)
- OBUs should be able to refill their anonymous certificate set (e.g., at traffic light or at gas station using a high speed connection)
- improved privacy, but …
  - limited protection against insider (class 4) attackers
  - changing pseudonyms is an effective mechanism only if the adversary's observational capabilities are limited (no global eavesdropping)
    → see study of effectiveness later

Anonymous self-enforcing certificates

- each OBU has a long-term symmetric key, which is used to authenticate the OBU when obtaining certificates from the CA
- certificate issuance
  - OBU generates k key pairs
  - CA blindly signs all k public keys
  - each key is valid only for one day
- problems
  - how to enforce the validity period?
    - CA can use different keys for different days
  - how to identify and revoke bad OBUs?
    - in case of DSA or ECDSA, the private key is selected randomly and the public key is computed from that
    - let the private key contain the identifier of the OBU
    - if a private key is compromised, then the OBU is identified, and no more certificates are issued to it

Anonymous self-enforcing certificates

- further problems
  - how to ensure that OBUs follow the protocol and put their ID in their private keys?
    - we can use a ***cut-and-choose technique***
    - each OBU generates 2k key pairs and the corresponding blinded unsigned certificates (two certificates for each day)
    - $(C'_{11}, C'_{12}), (C'_{21}, C'_{22}), \ldots, (C'_{k1}, C'_{k2})$ are sent to the CA
    - the CA randomly selects one cert from each pair and the OBU must unblind those blinded certificates and reveal the corresponding private keys
    - if at least one private key is badly formatted, the OBU is revoked
    - otherwise, the CA signs the other element of each pair
    - the probability that n badly formatted key is certified is 2^{-n}
- advantages
  - privacy is fully protected
  - short certificate life-time → no need for CRLs
- disadvantage
  - short certificate lifetime → large overhead of obtaining certificates
  - anonymity cannot be revoked based on signed messages only

Group signatures

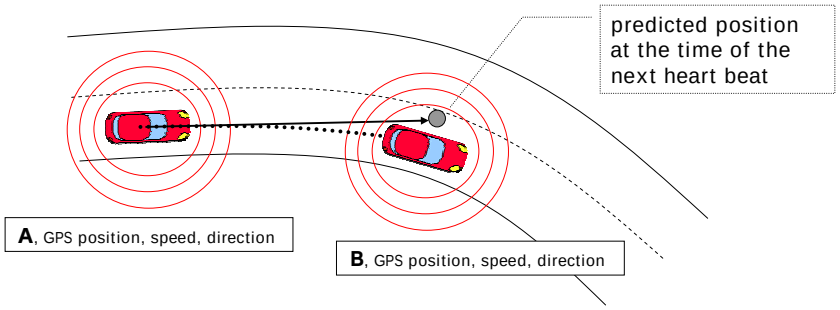
- operation
  - a group signature scheme has a single public key and a large number of private keys
  - a signature that is generated with any of the private keys can be verified with the public key
  - verifier learns only that the message was signed by a member of the group, but cannot tell which member
- all vehicles from the same country can form a group
- elegant but not very efficient yet
- could possibly be combined with anonymous certificates
  - vehicles can use a group signature scheme to issue pseudonyms for themselves (this would be done by a trusted hardware security module (HSM) in each vehicle)
  - a receiver may receive several messages signed under the same pseudonym (within the lifetime of a pseudonym), but needs to verify the group signature on corresponding certificate only once

  → efficiency of standard pseudonyms is retained

  → problem of running out of pseudonyms is eliminated

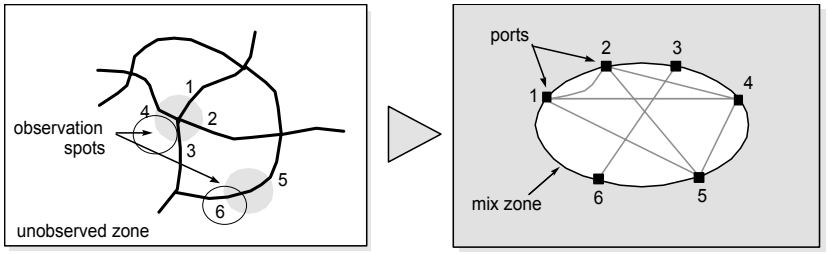
Effectiveness of changing pseudonyms

- changing pseudonyms is ineffective against a global eavesdropper



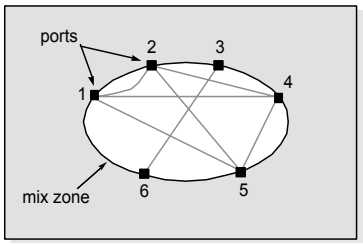
- hence, the adversary is assumed to be able to monitor the communications only at a limited number of places and in a limited range

The mix zone concept



- the unobserved zone functions as a *mix zone* where the vehicles change pseudonym and mix with each other
- note that the vehicles do not know where the mix zone is (this depends on where the adversary installs observation spots)
- we assume that the vehicles change pseudonyms frequently so that each vehicle changes pseudonym while in the mix zone

Model of the mix zone



- we assume that the adversary knows
  - q_{ij} - the conditional probability of exiting the mix zone at port j given that the entry port was port i (for all i, j)
  - $f_{ij}(t)$ – the (discrete) probability distribution of the delay when traversing the mix zone between ports i and j

Tracking strategy of the adversary

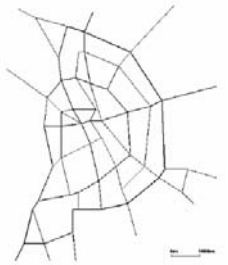
- the adversary observes entering and exiting events, and wants to relate them to each other
- more specifically, the adversary
  - picks a vehicle v in the observed zone
  - tracks v until it enters the mix zone at port s
  - then, observes the exiting events until time T (where the probability that v leaves the mix zone until T is close to one)
  - for each exiting vehicle at port j and time t, computes $p_{jt} = q_{sj} f_{sj}(t)$
  - the adversary decides to the exiting vehicle v' for which p_{jt} is maximal
  - the adversary is successful if v' = v
- this algorithm realizes a Bayesian decision
  - it minimizes the error probability of the decision
  - in this sense, it is optimal

Privacy metric

- the level of privacy achieved is characterized by the success probability of the adversary
  - if success probability is high, then level of privacy is low
- how to determine it?
- we used simulations to determine its empirical value in realistic scenarios

Simulation settings

- we generated a simplified map of Budapest with MOVE
- we generated movement of the vehicles on the map with SUMO
  - low traffic: 250 new vehicles / time step
  - medium traffic: 500 new vehicles / time step
  - high traffic: 750 new vehicles / time step
- we selected the adversary's observation spots in intersections of roads
  - number of observation spots were varied from 5 to 59 with a step size of 5



Simulation settings

- we let the adversary build her model of the mix zone by letting her fully tracking vehicles for some time
- after that, we let the adversary pick a vehicle, track it until it enters the mix zone, observe exiting vehicles, and make a decision
- we run 100 simulations for each simulation setting
- we look at the percentage of the simulation runs where the adversary is successful

Simulation results