# Securing Vehicular Communications

Panos Papadimitratos
panos.papadimitratos@epfl.ch

Jean-Pierre Hubaux
jean-pierre.hubaux@epfl.ch

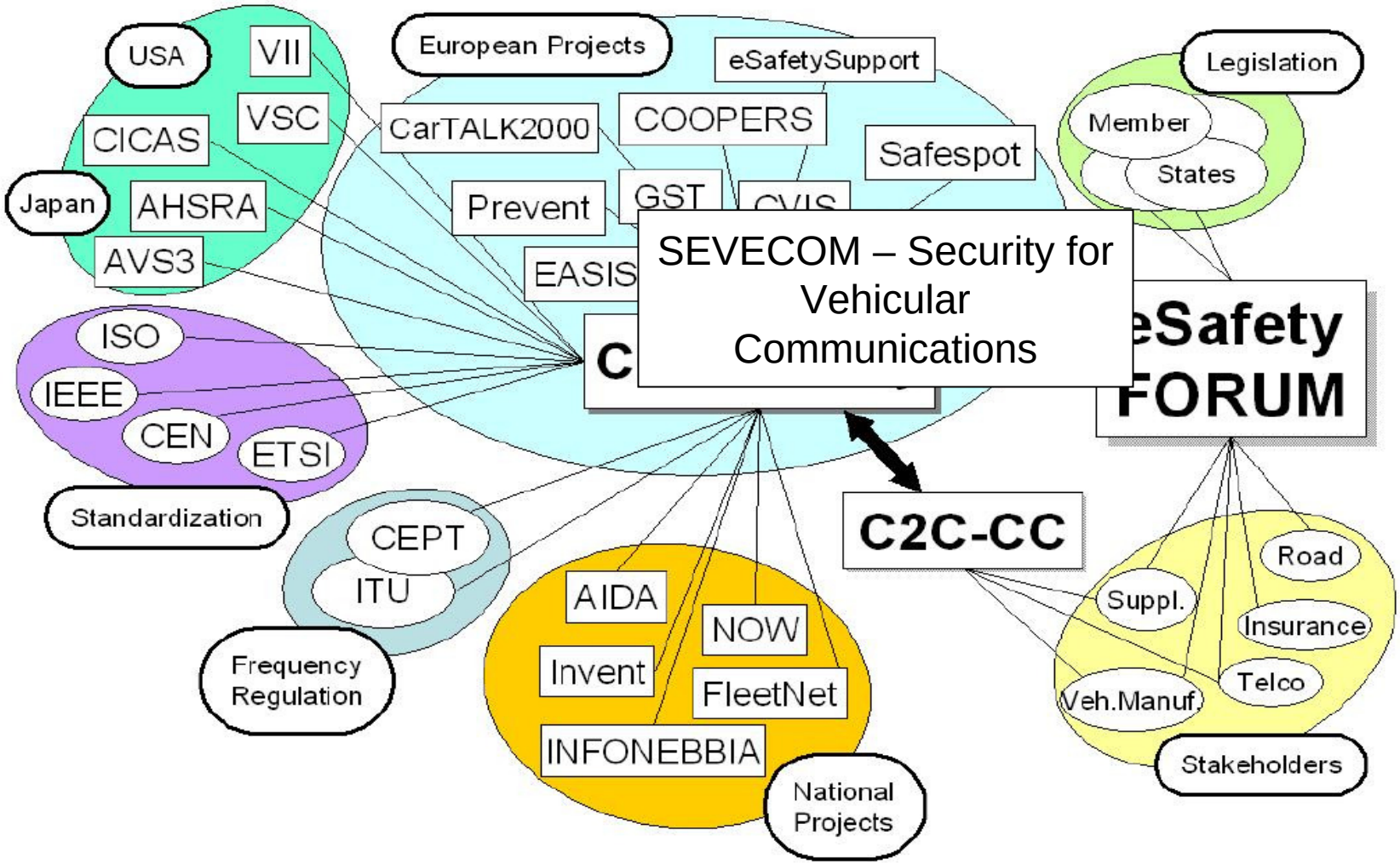
Laboratory for computer Communications
and Applications (LCA)

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

# Vehicular Communications (VC)

- Technology in the making
  - Mobile Ad Hoc Networking
    - Vehicular Ad Hoc Networks (VANET)
  - Infrastructure-based wireless communications
- Eventually wide, gradual deployment
- Interoperability
- Standardization

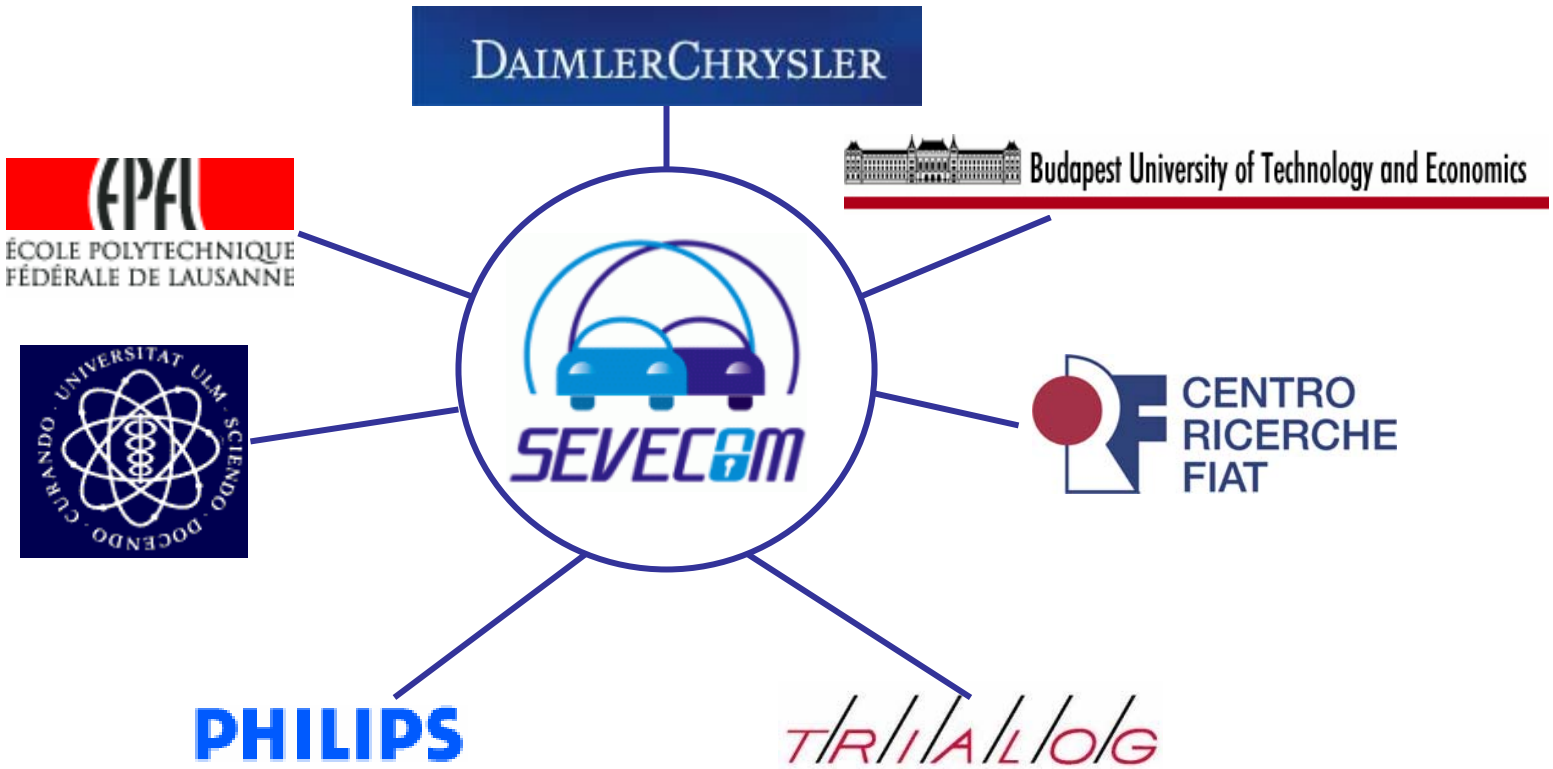
# VC Technology Development
# Research and Standardization




*Slide courtesy of Antonio Kung*

# European Project: SeVeCom

- SeVeCom: Secure Vehicular Communications
- http://www.sevecom.org
- Started January 2006; Duration: 3 years; Total budget: 3 MEuros




*Slide courtesy of Maxim Raya*

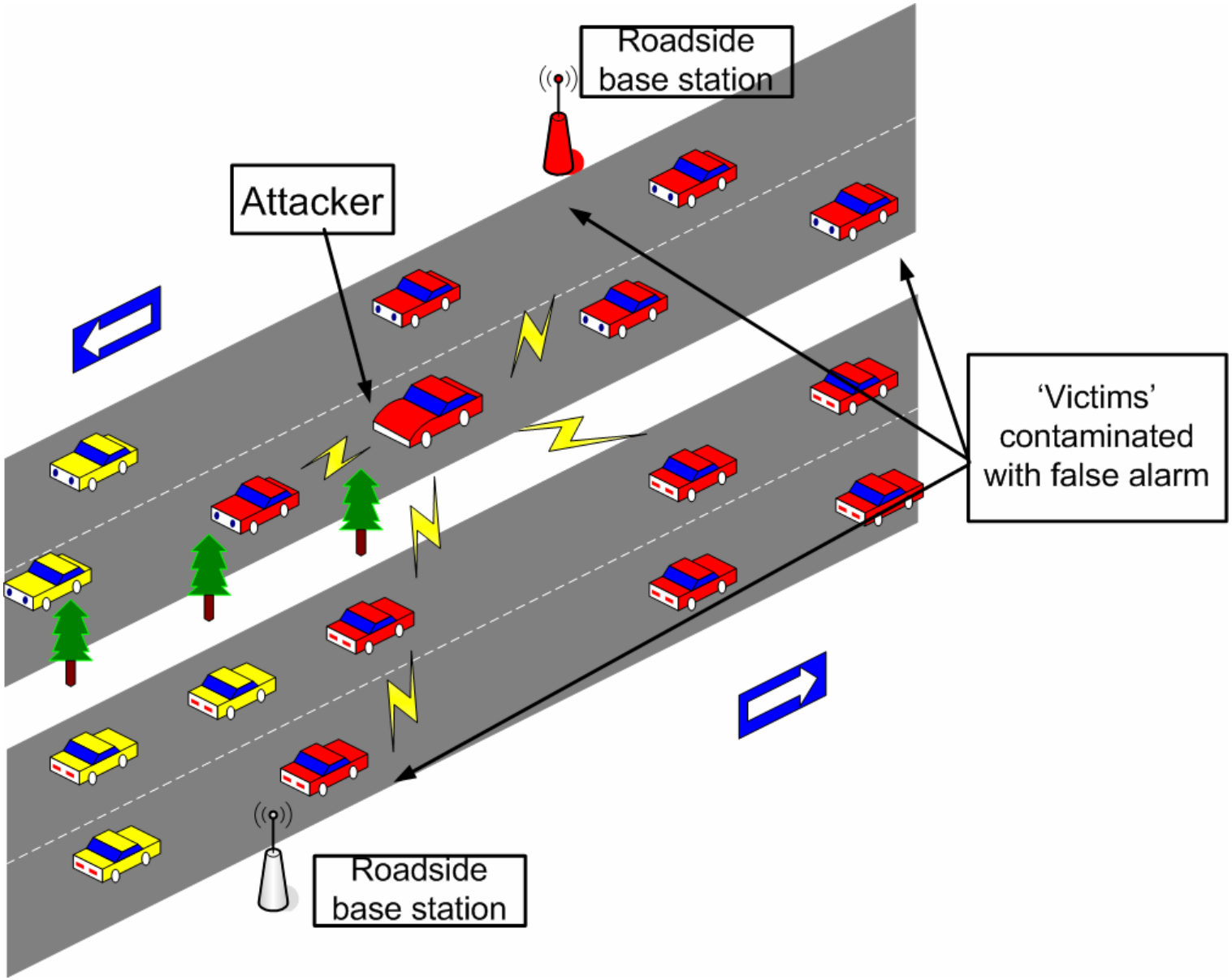
Safety

Information Society and Media

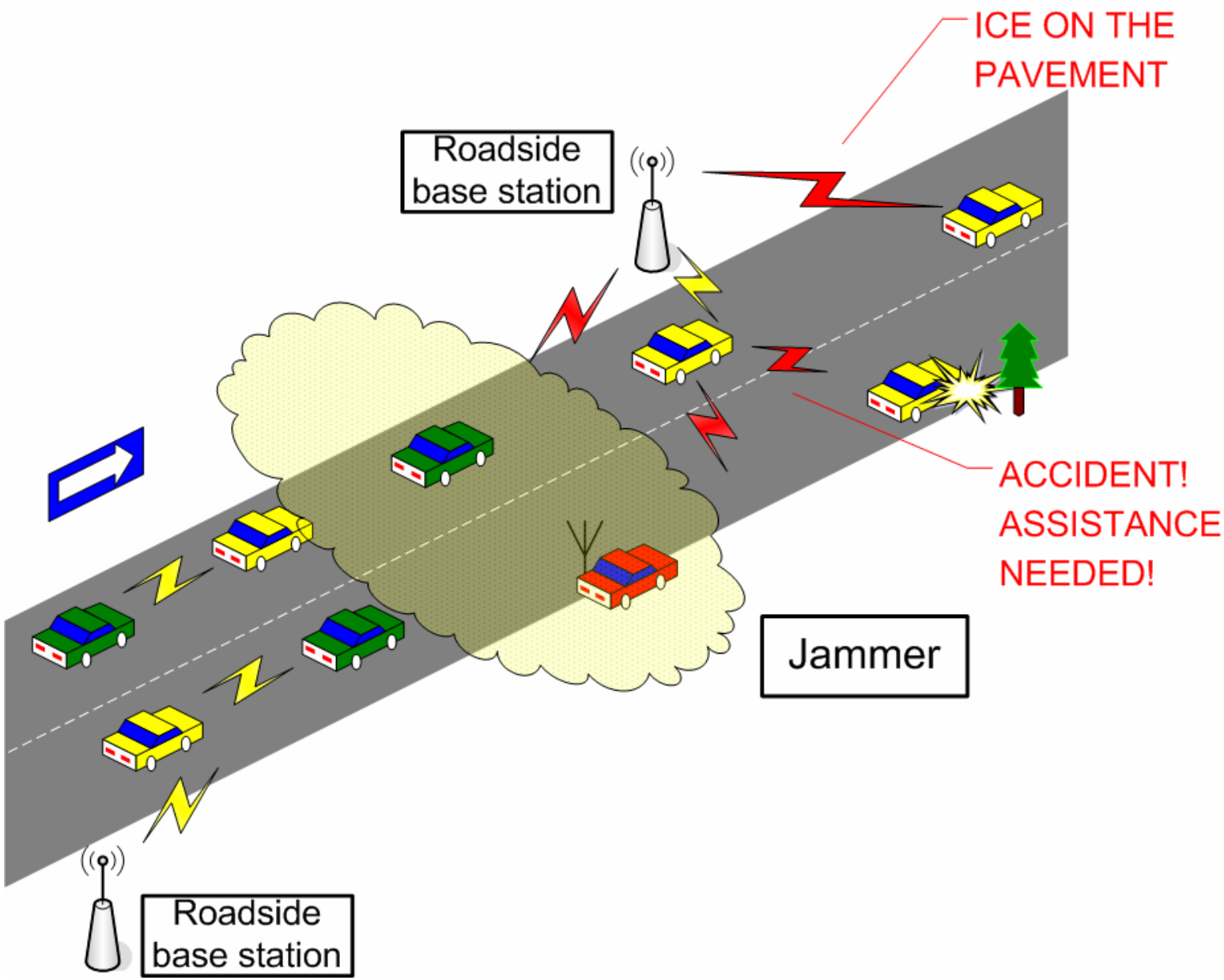
# Security and Privacy – Why?

- Without robust designs, VC systems may facilitate antisocial behavior
- The deployment of vulnerable VC systems may cancel out their envisioned benefits
- Abused, poorly defended VC systems can cause damages and high cost
- Attackers and adversaries will always be present

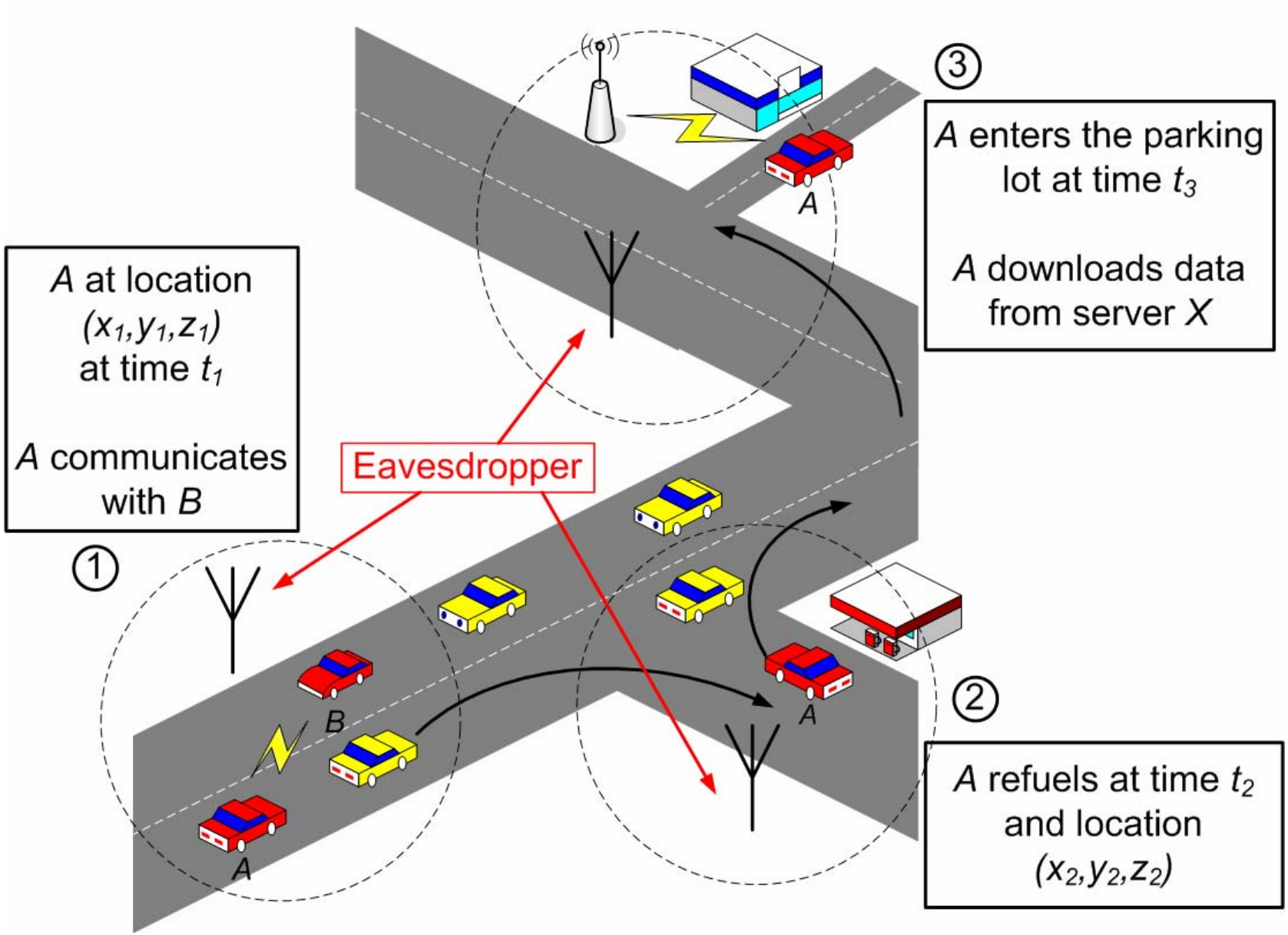
# Attacks and Exploits
## *Example 1*: Inject false information



# Attacks and Exploits
## *Example 2*: Denial of Service



# Attacks and Exploits
## *Example 3*: Vehicle and User Tracking



# Security System Requirements

- Message Authentication and Integrity
  - Messages must be protected from any alteration and the receiver of a message must corroborate the sender of the message
- Entity authentication
  - The receiver is ensured that the sender generated a message *recently*
- Message Non-Repudiation
  - The sender of a message cannot deny having sent a message

# Security System Requirements (cont'd)

- Access control
  - Distinct roles for different types of network entities
  - Regulate access to information/services
  - *Authorization:* Establish what each network entity is allowed to do (e.g., protocols to run, messages to send)
- Message Confidentiality
  - The content of a message is kept secret from those nodes that are not authorized to access it

# Security System Requirements (cont'd)

- Privacy - Anonymity
  - *VC* systems should not disclose or allow inferences on the personal and private information of the users
  - At *minimum*, an observer can*not* learn if a node performed, or will perform in the future, a specific action, assuming that the node performs the action
- Full anonymity
  - For an observer, an action could have been performed by any other entity in the system

# Security System Requirements (cont'd)

- Availability
  - Protocols and services should remain operational even in the presence of faults, malicious or benign
  - Secure and fault-tolerant designs
  - Resilience to resource depletion attacks
  - Self-stable protocols

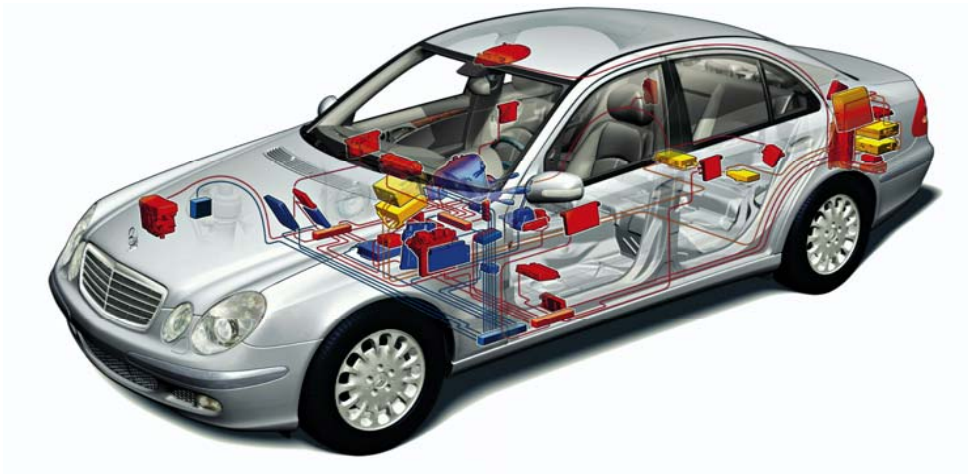
- Liability
  - Users of vehicles are liable for their deliberate or accidental actions that disrupt the operation of other nodes, or the transportation system
  - The VC system should provide information that assists the attribution of liability
  - Auditing

# Onwards to Secure VC Systems

- Point of caution
  - Not all requirements listed here are relevant to all applications and scenarios
- System model
- Adversary model
- Security architecture building blocks

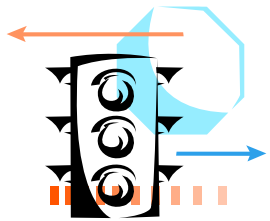
# System Model

- Vehicles
  - Private
  - Public
- Complex in-car system
- Abstract view
  - Central processing and communication module
  - Unique identity *V*
  - Credentials and cryptographic keys

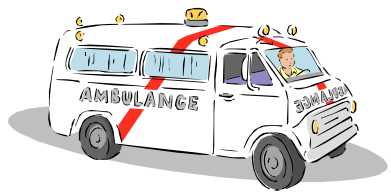


*Graphic courtesy of DC*

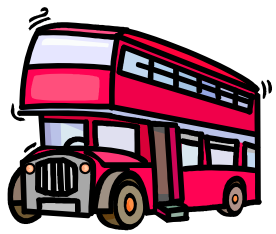
# System Model (cont'd)



- Infrastructure
  - Roadside units
    - VC base stations
    - Varying complexity




- Public vehicles
  - Emergency, police, buses



- Special roles and attributes
  - Relatively more trustworthy
  - Facilitate security-related operations

# Adversary Model

- Any wireless device that implements a rogue version of the VC protocol stack can be an adversarial node
- Internal adversaries equipped with the system credentials
- Adversaries can forge and inject any message, modify in-transit messages, replay any received message

# Adversary Model (cont'd)

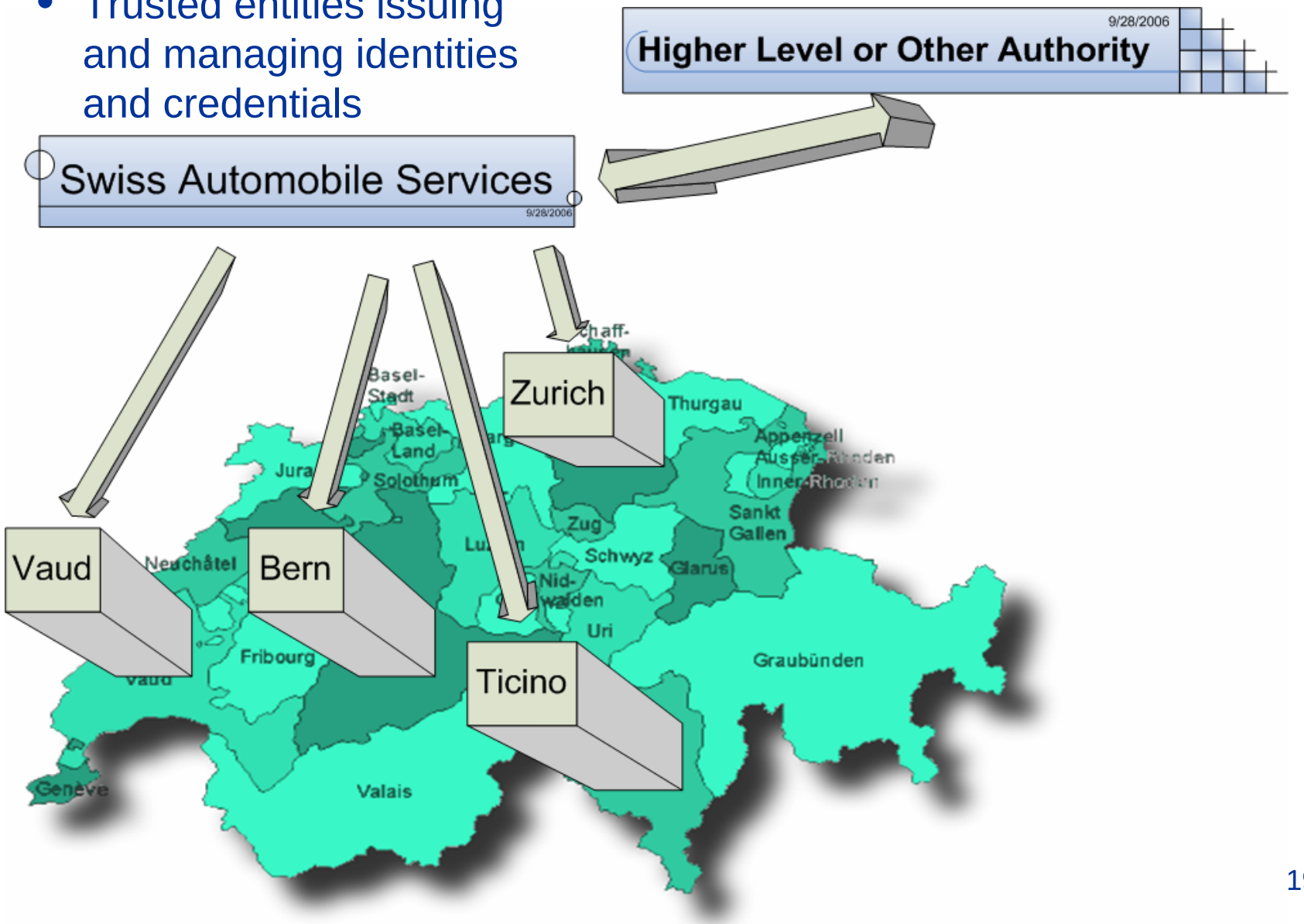
- Input controlling adversary
  - Tamper with sensory inputs
  - Much easier that hacking with the VC system software
  - Control the node's behavior
- Adversarial parsimony
  - A small number/fraction of adversaries are more likely than a large number to be present in a network area
  - Adversaries are more likely to be independent than colluding

# What makes VC and their security different?

- Complexity of the system
  - Hybrid (ad hoc, infrastructure) networking
  - Sensory inputs
- Tight coupling between users, applications, and network
- Pre-VC transportation systems and ‘legacy’ constraints and requirements
  - Liability identification
- Large scale and high mobility
- Stronger privacy concerns

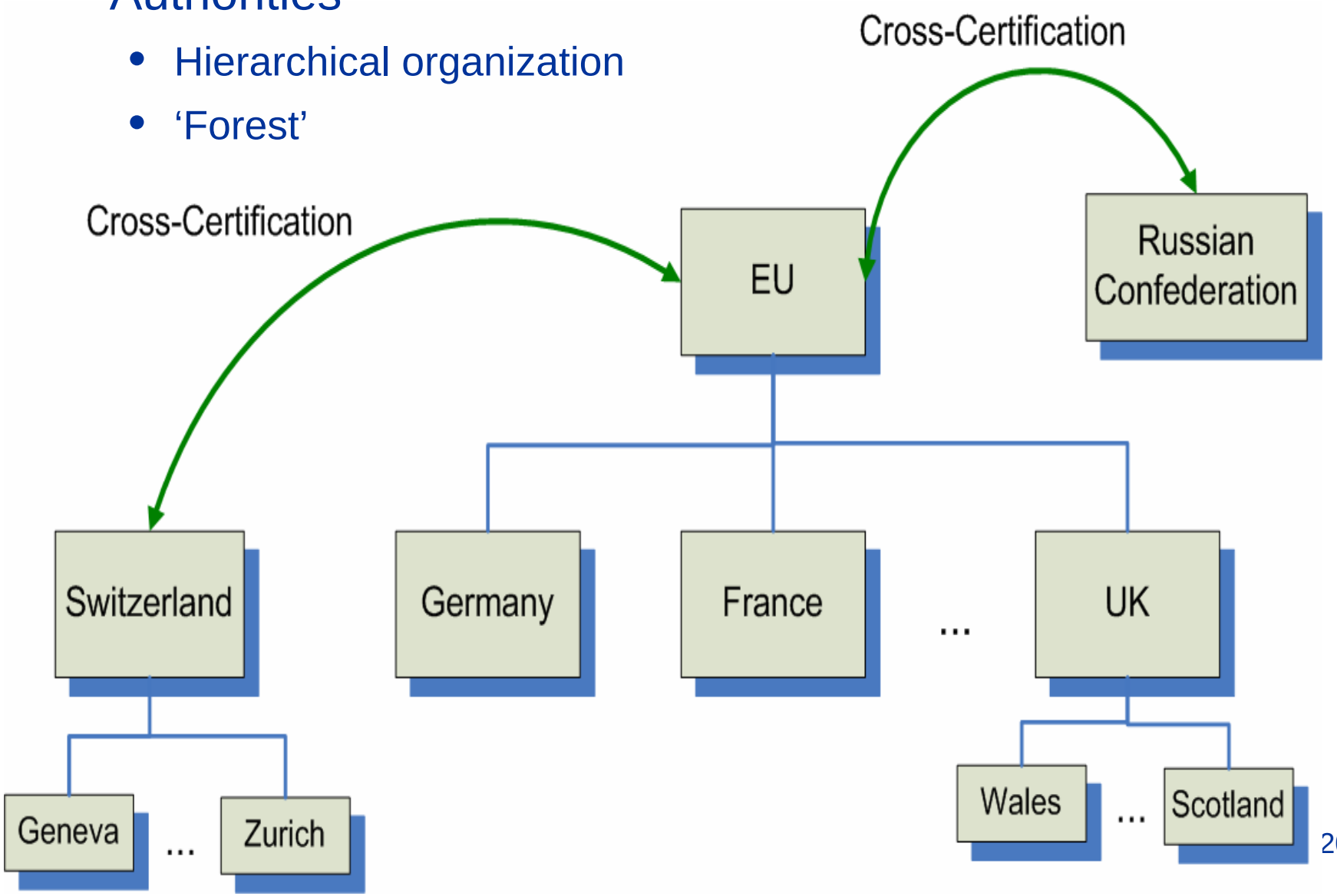
# Secure VC Building Blocks

- Authorities
  - Trusted entities issuing and managing identities and credentials



# Secure VC Building Blocks

- Authorities
  - Hierarchical organization
  - ‘Forest’

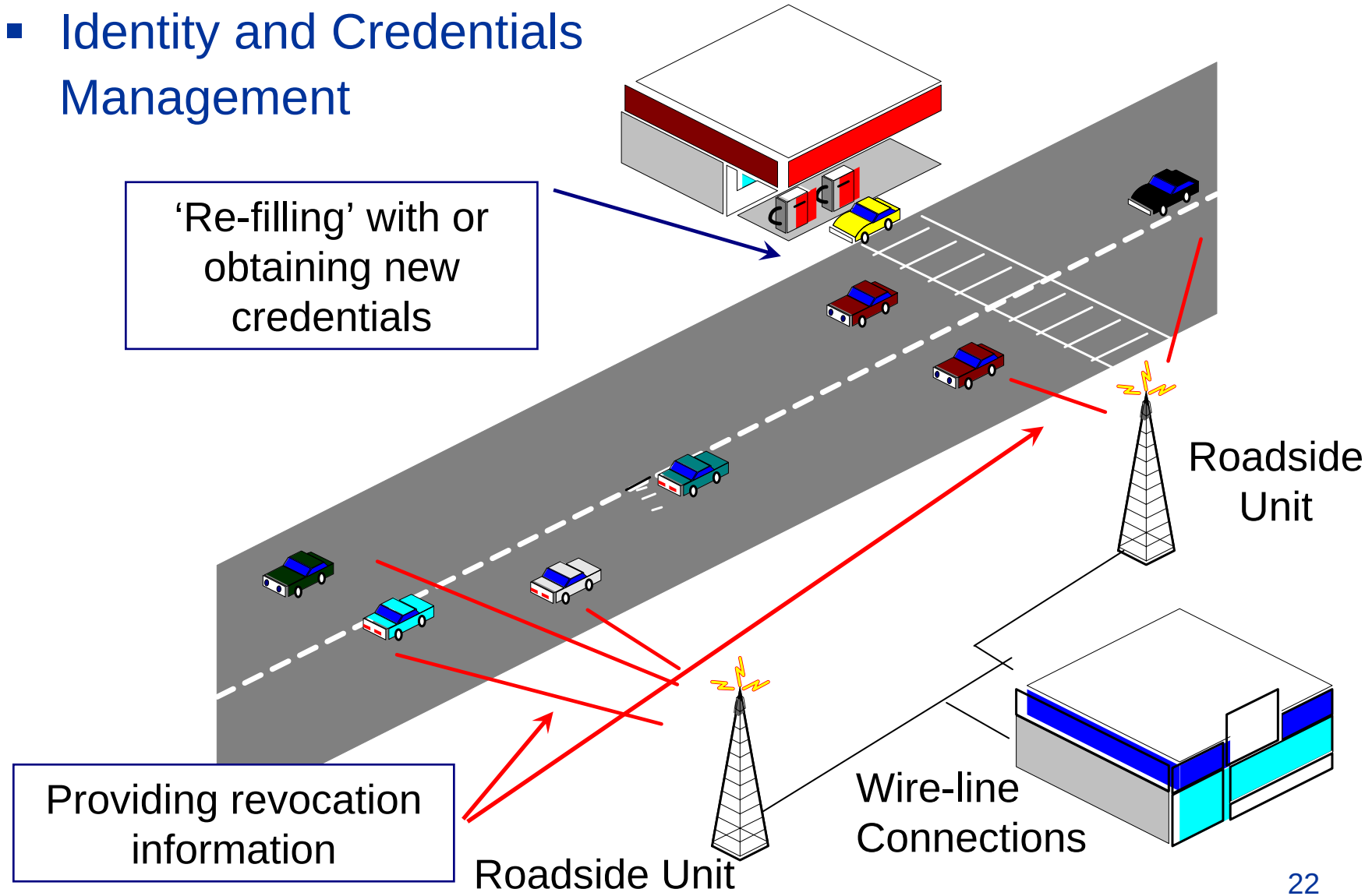


# Secure VC Building Blocks

- Each node
  - Unique identity *V*
    - Integration of pre-VC and VC-specific identifiers
  - Public / private key pair
    - $K_V$, $k_V$
  - Certificate
    - $Cert_X\{K_V, A_V\}$
    - $A_V$: attributes of node *V*
- Multiplicity of service providers granting credentials
- Alternative implementations for identification; *manufacturers?*

# Secure VC Building Blocks (cont'd)

- Identity and Credentials Management

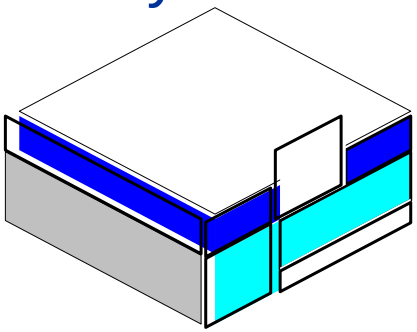


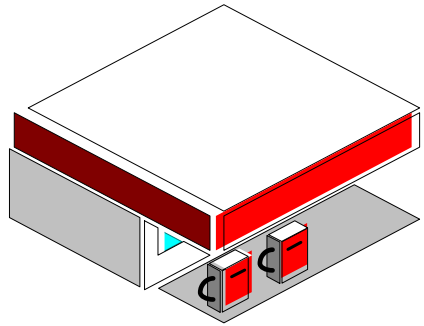
# Secure VC Building Blocks (cont'd)

- Secure Communication
  - Single- and Multi-hop
  - Vehicle to vehicle
  - Vehicle to infrastructure
- Digital signatures more appropriate tool
  - Any to any communication; e.g., broadcast, geo-cast
  - High mobility
- Relatively simple networking protocols 'shift' the security focus to the application

# Secure VC Building Blocks (cont'd)

- Privacy enhancing technologies





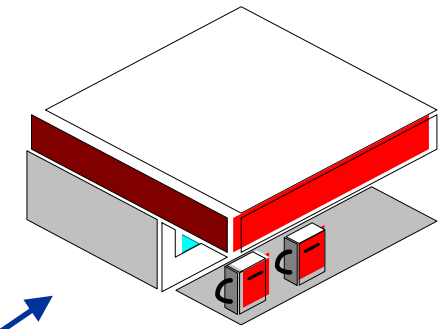
- Authority *X*
  - Provides $Cert_X\{K_V, A_V\}$ to the vehicle *V* with public key $K_V$ and attributes' list $A_V$
  - $K_X$ own public key

- Authority *A*
  - Issues credentials for anonymous authentication
  - $K_A$ own public key

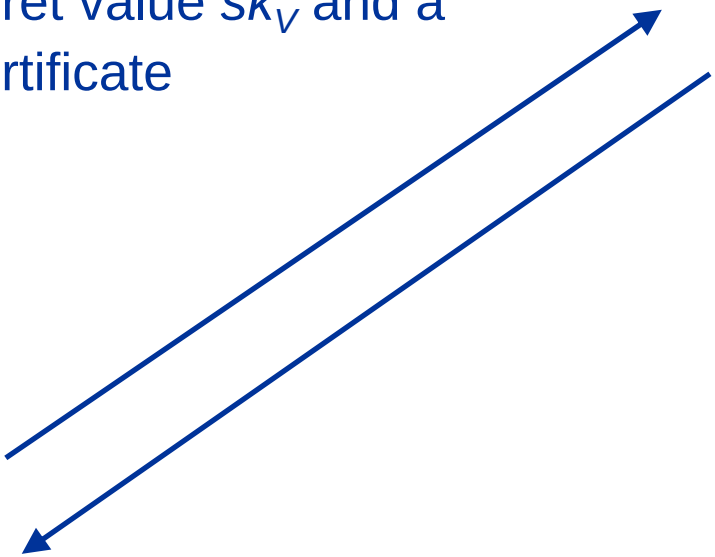
- Vehicle *V*
  - $K_V, k_V$
  - $Cert_X\{K_V, A_V\}$
  - $K_X$, $K_A$

# Secure VC Building Blocks (cont'd)

- *Join*
  - Interactive protocol
  - *V* becomes a member of group $G_A$
  - *V* obtains a secret value $sk_V$ and a membership certificate



- Authority *A*



- There is a single public key for $G_A$

- Vehicle *V*

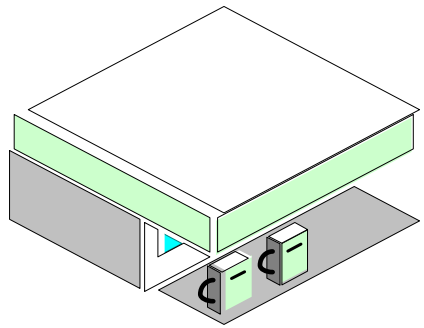
# Secure VC Building Blocks (cont'd)

- *Sign/show*
  - The vehicle uses its secret and membership
- *Verify*
  - Any receiving vehicle/roadside unit
    - Validates the signature with respect to $G_A$
    - Verifies (or not) that the message originates from a legitimate (i.e., not revoked or expired) member of $G_A$

# Secure VC Building Blocks (cont'd)

- *Open* – Anonymity revocation

Anonymous communication transcript

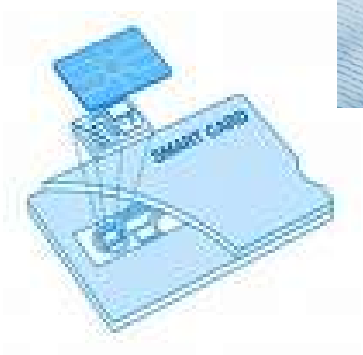


Authority *O*

"Vehicle *V* generated the transcript"

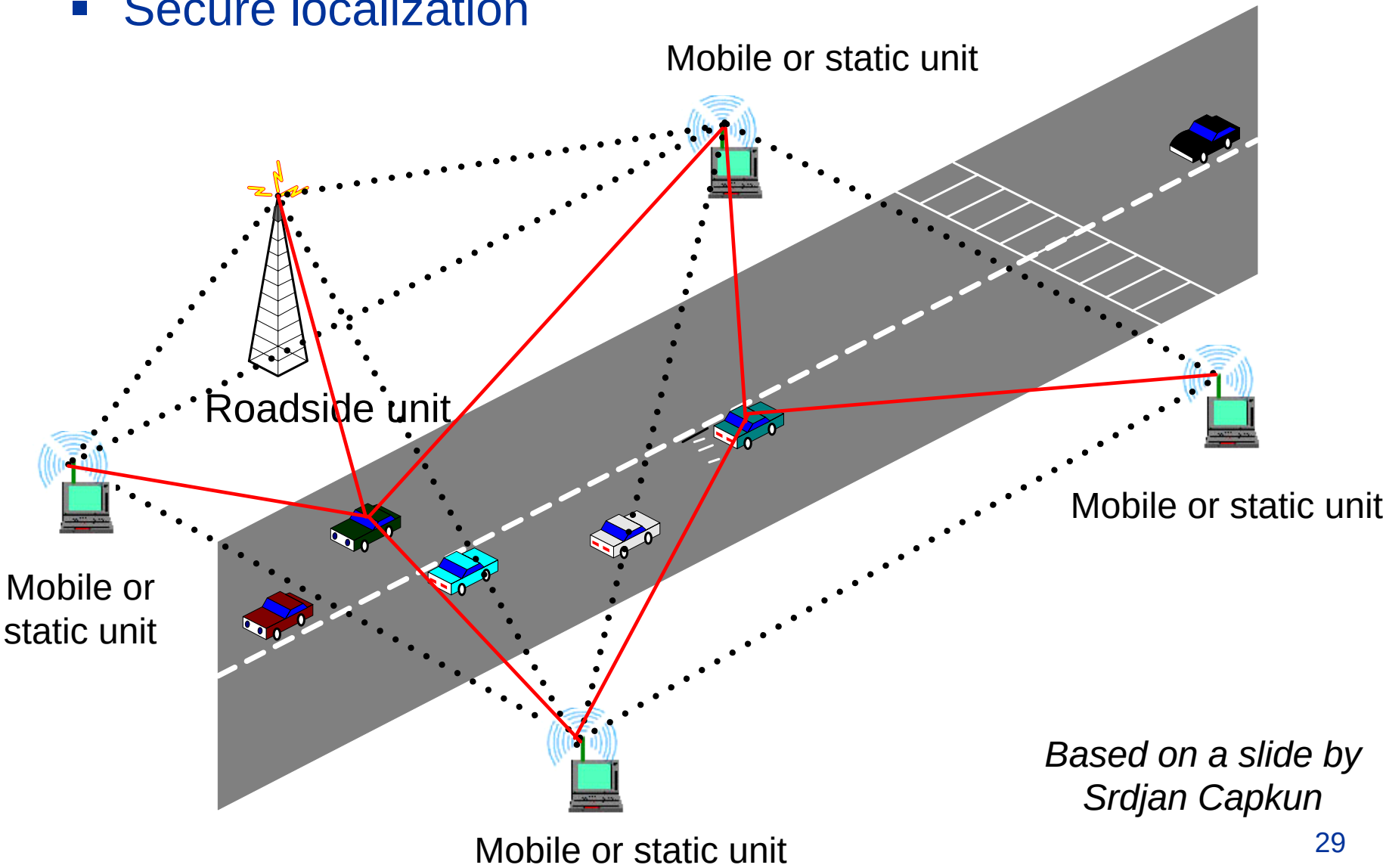
# Secure VC Building Blocks (cont'd)

- Trusted on-board components
  - Tamper-resistant
  - Storage
    - Cryptographic material
    - Data
  - Processing
    - Cryptographic operations
  - Motivation
    - Current state; Event Data Recorders (EDRs)
    - Bind physically cryptographic material to the vehicle



# Secure VC Building Blocks (cont'd)

- Secure localization

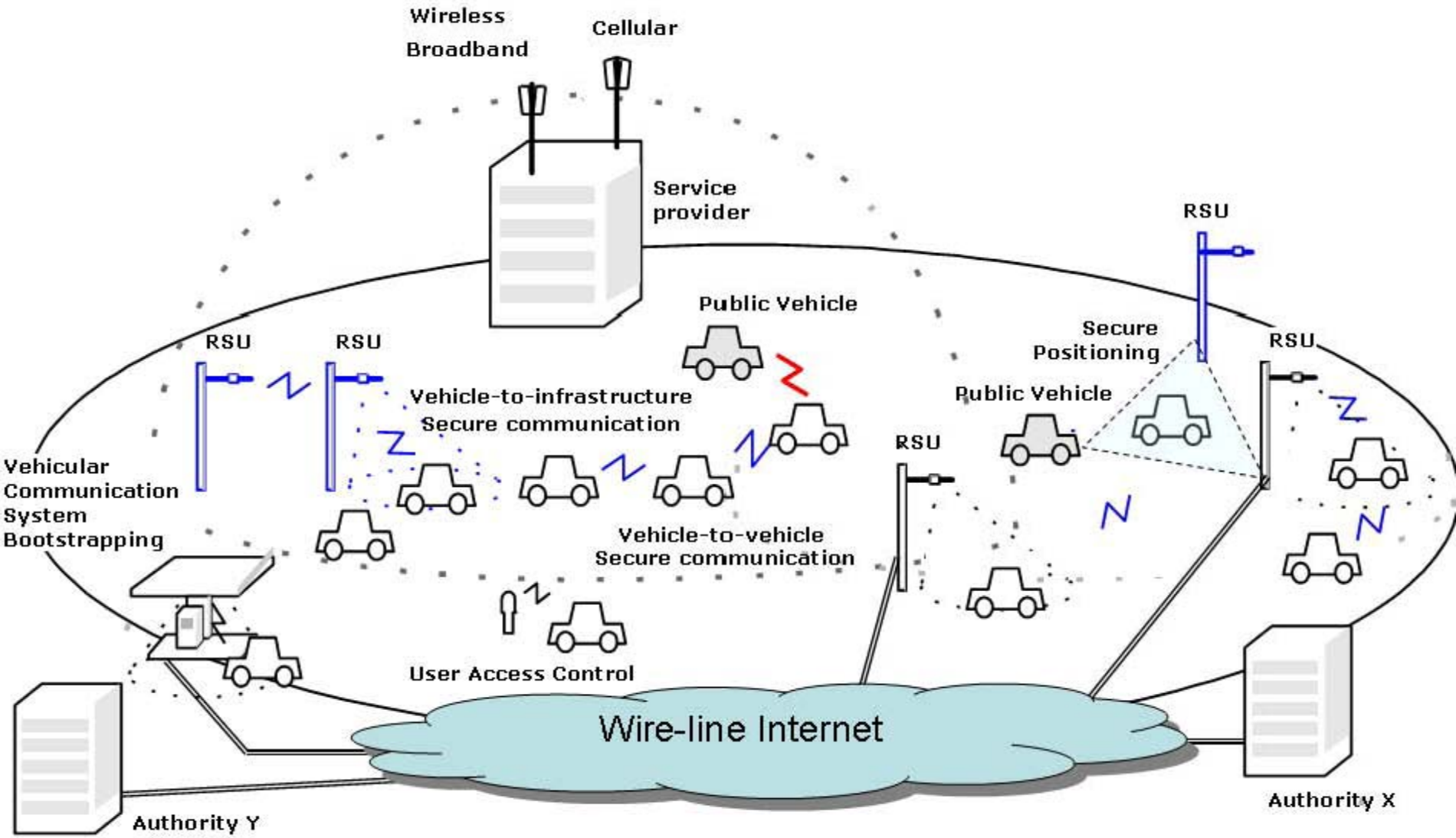



*Based on a slide by Srdjan Capkun*

# Secure VC Building Blocks (cont'd)

- Other issues
  - Resilience to false measurements/data
    - Data consistency
  - In-car security
  - User identification
  - Secure user interface
  - User-vehicle association

# Secure VC Architecture Overview
# An Illustration



# Conclusions

- Security and privacy-enhancing mechanisms are a prerequisite for the VC systems deployment
- Securing VC systems is a complex yet ‘real’ problem that attracts the attention of the community
- Opportunity: Awareness and joint efforts in industry and academia

- More information, related and upcoming publications:
  - *http://ivc.epfl.ch*
  - *http://www.sevecom.org*