Secure Vehicle Communication

SEVECOM (SE-cure VE-hicle COM-munication)

Presentation

Antonio Kung

SEVECOM Coordinator

Trialog

25 rue du Général Foy, 75008 Paris

Tel: +33 1 44 70 61 00

www.trialog.com

Safety

Information Society and Media

Outline

- Context
- Objectives
- Example attacks
- Research topics
- Work Packages and Timetable
- Liaison with other eSafety projects/initiatives
- Conclusion

SE-cure VE-hicle COM-munication

- Mission: future-proof solution to the problem of V2V/V2I security

- IST STREP Project. 1/1/2006-1/1/2009
- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Riserche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

Partners

DaimlerChrysler

Centro Ricerche Fiat

EPFL École Polytechnique Fédérale de Lausanne

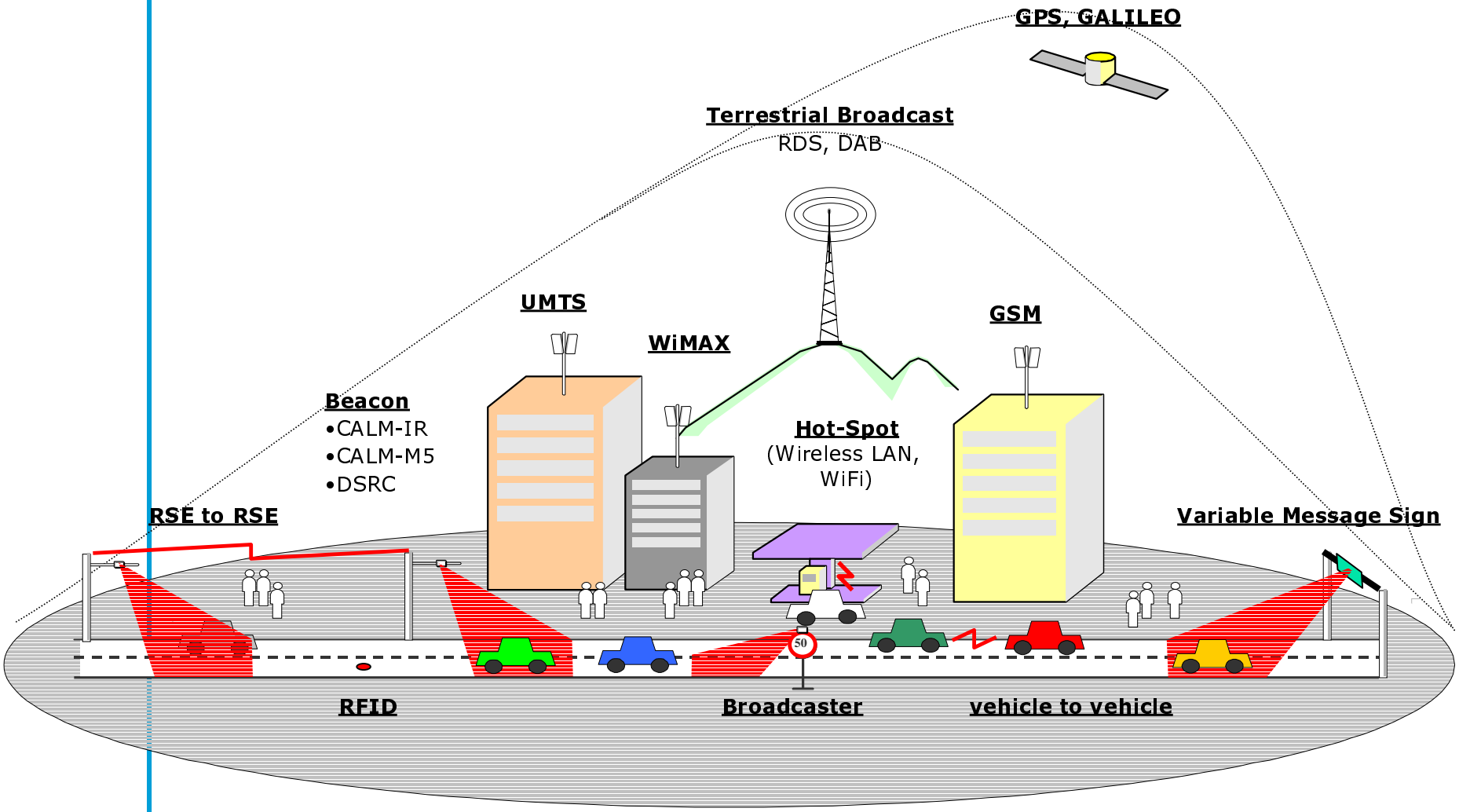
Philips

Trialog

Universität Ulm

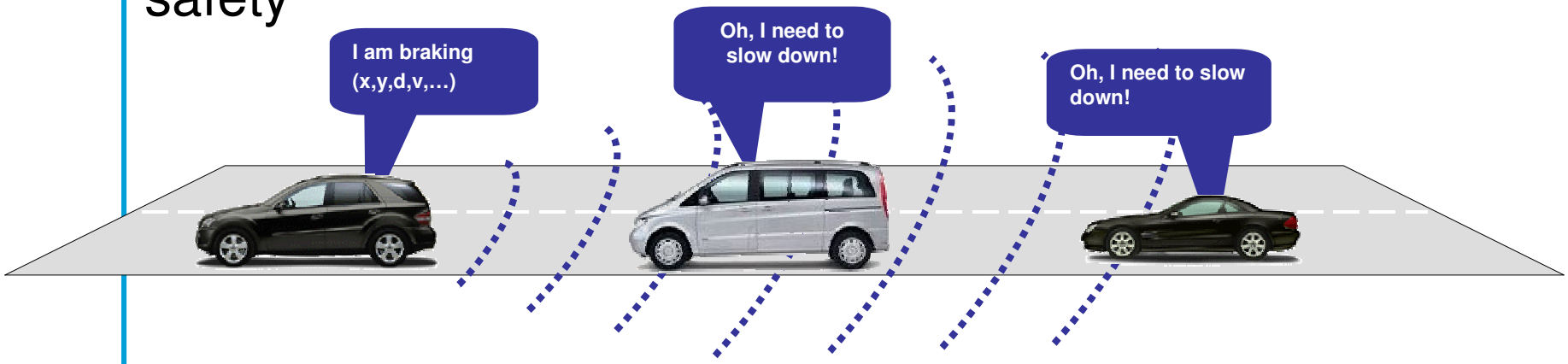
Budapest University of Technology and Economics

V2V and V2I Infrastructure

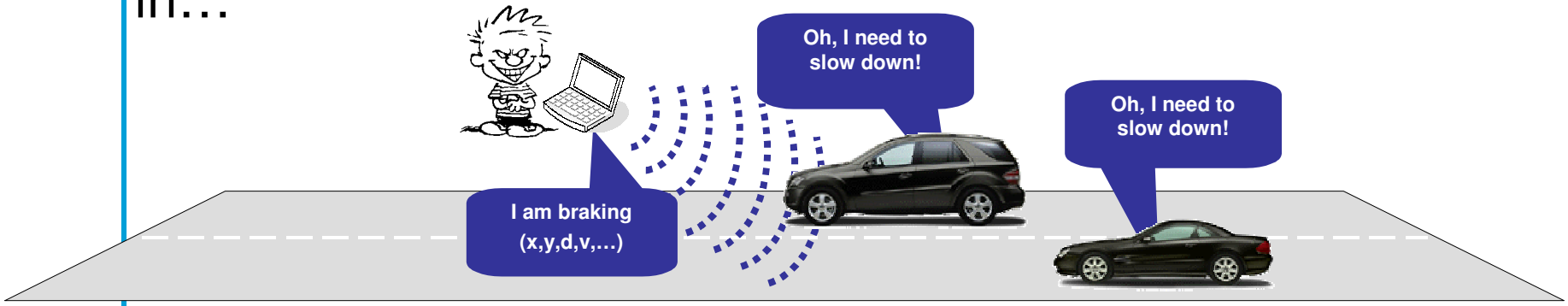


V2V Communication - Trust

- Sharing information among vehicles helps to improve safety

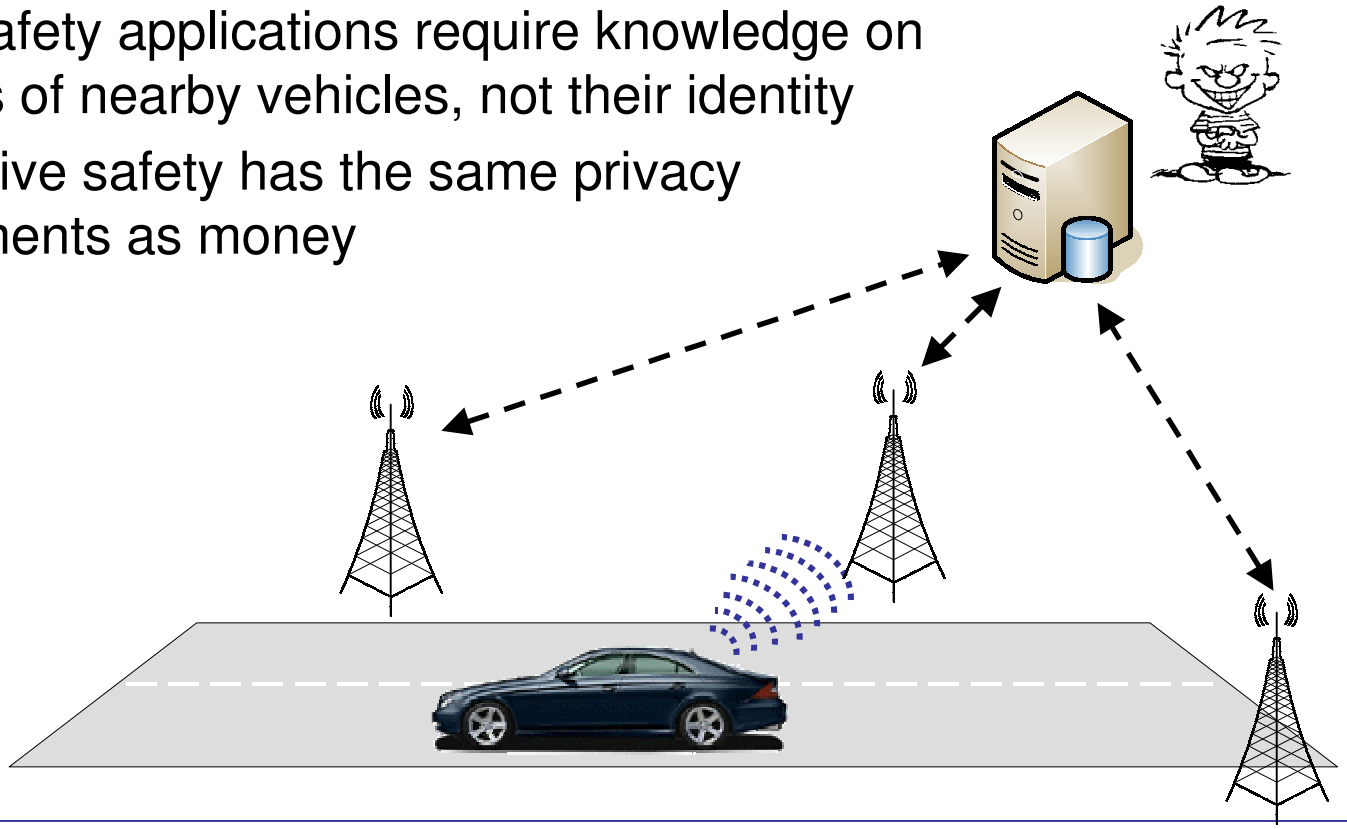


- However, inadequate security support could easily result in…



V2I Communication - Privacy

- V2V / V2I communication
  - should not make it easier to identify or track vehicles
  - should conform to future privacy directives
- Lack of privacy control will prevent deployment
  - Active safety applications require knowledge on activities of nearby vehicles, not their identity
  - Automotive safety has the same privacy requirements as money

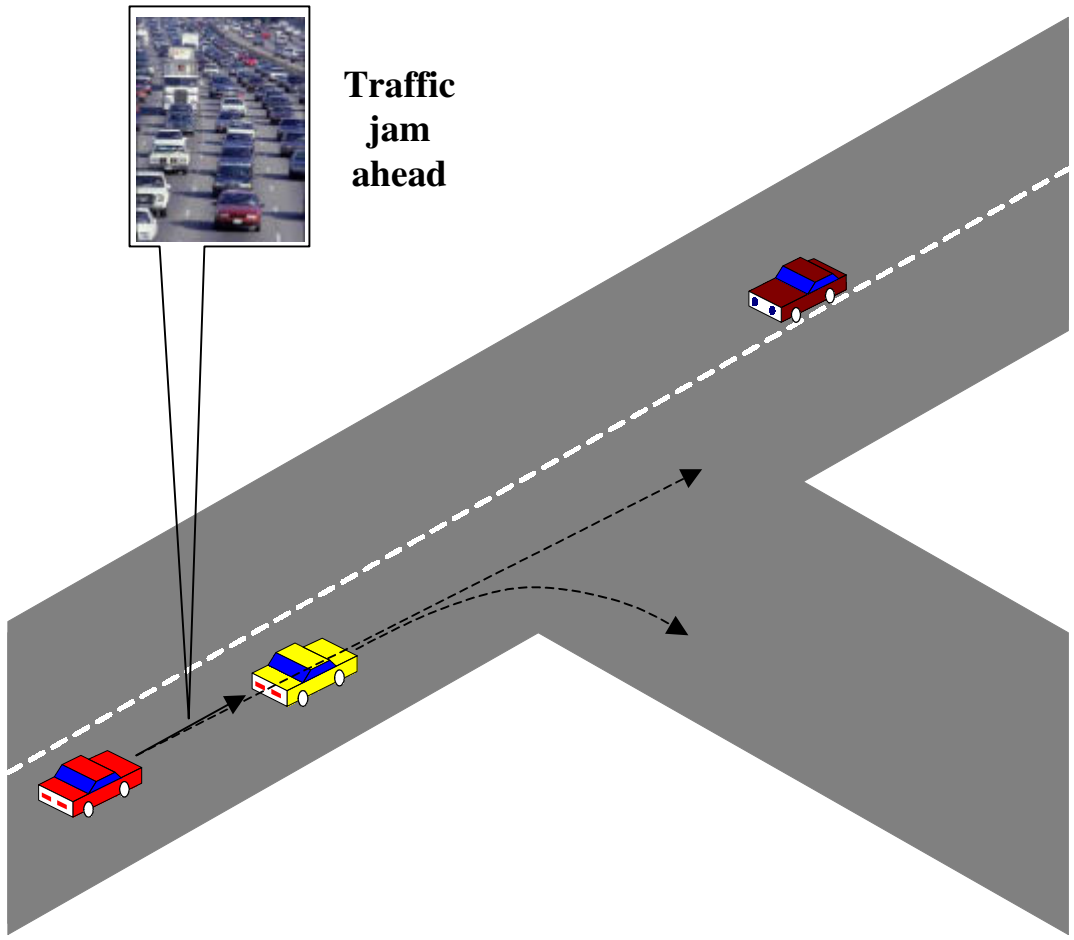


Objectives

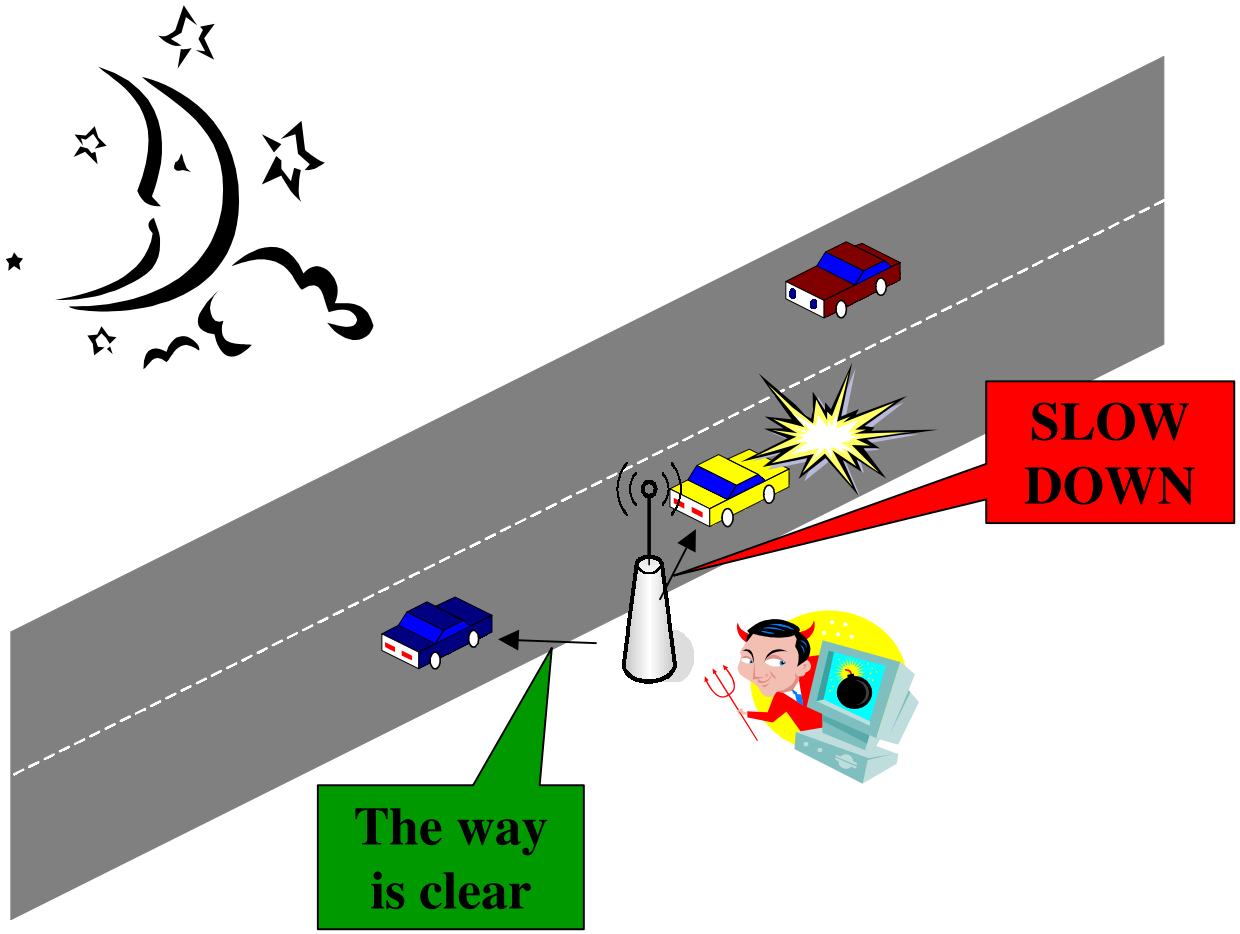
SEVECOM

- Large projects have explored vehicular communications
  - Fleetnet, PATH (UC Berkeley),…
- No solution can be deployed if not properly secured
- The problem is non-trivial
  - Specific requirements (speed, real-time constraints)
  - Contradictory expectations
- SEVECOM will focus on:
  - Identification of threats against the radio channel, transferred data, and the vehicle itself
  - Specification of a security architecture
  - The definition of suitable cryptographic primitives

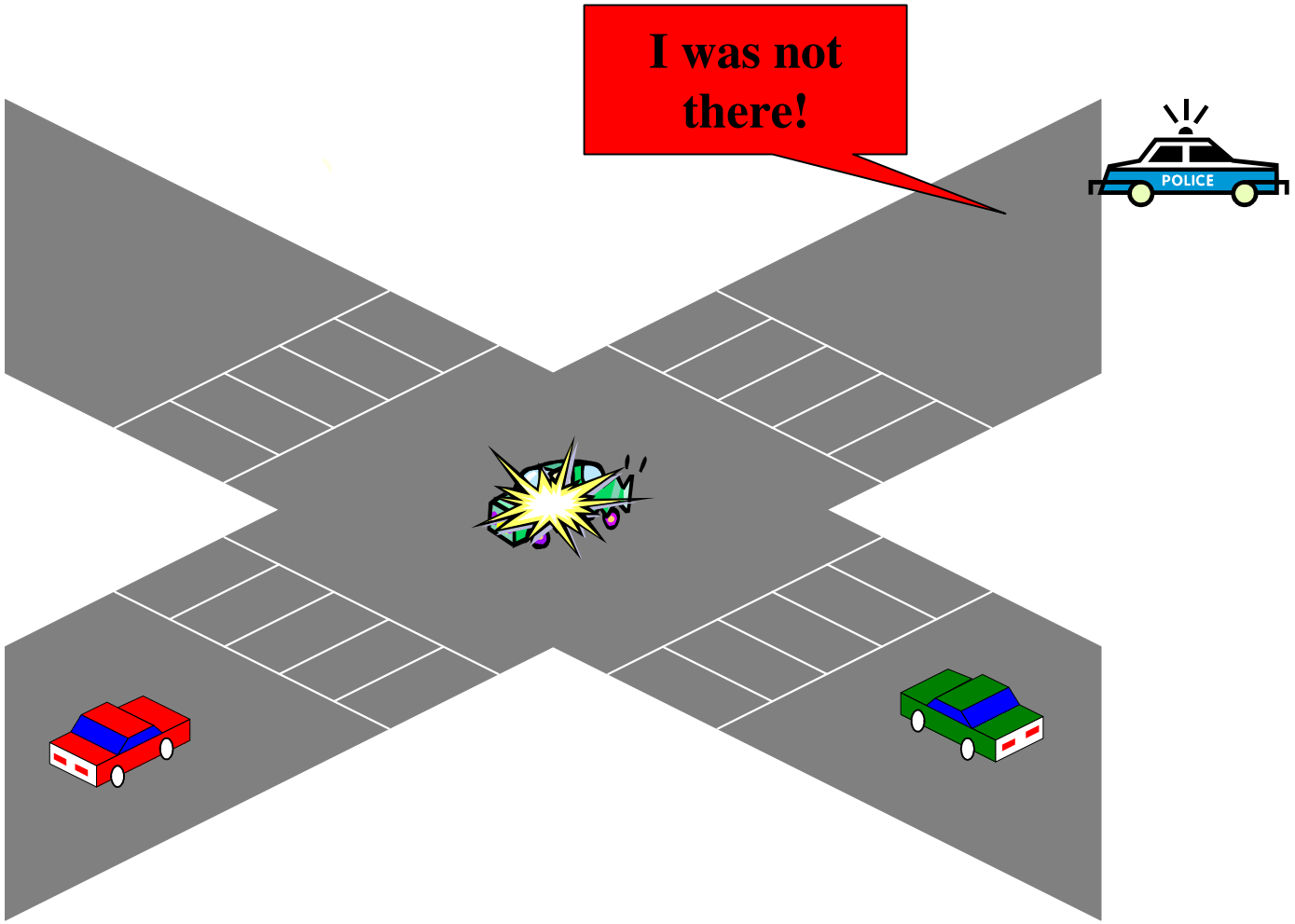
Example attack 1 : Bogus traffic information



Example attack 2 : Disruption of network operation



Example attack 3: Cheating with identity, position or speed



Research topics

	Topic	Scope of work
A1	Key and identity management	Fully addressed
A2	Secure communication protocols (inc. secure routing)	Fully addressed
A3	Tamper proof device and decision on cryptosystem	Fully addressed
A4	Intrusion Detection	Investigation work
A5	Data consistency	Investigation work
A6	Privacy	Fully addressed
A7	Secure positioning	Investigation work
A8	Secure user interface	Investigation work

Work Packages

SEVECOM

- WP1: Requirements
- WP2: Architecture and Security Mechanisms Specification
- WP3: Focused Development and Integration into Selected Infrastructure
- WP4: Integration in Use Cases
- WP5: Approaches for Security Evaluation
- WP6: Liaison, Dissemination and Exploitation
- WP7: Project Management

WP2 – Task 1: *Security Architecture*

SEVECOM

- This task will specify the VC security architecture, taking into account A1 to A8

- The industrial partners will focus on industrial requirements:
  - suitability for integration in C2C technologies
  - genericity of approach to allow for evolution (e.g. switching from one security mechanism to another)
  - upward compatibility when different versions are deployed

WP2 – Task 2: *Analysis of Security Mechanisms*

SEVECOM

- This task will focus on:
  - Key and identity management (A1)
  - Secure communication protocols (inc. secure routing) (A2)
  - Tamper proof device and decision on cryptosystem (A3)
  - Privacy (A6)
- Define formal models of the protocols in Task 1 and analyze their security features
- Evaluate the security of the implemented versions of the protocols

WP2 – Task 3: *Specification of Security Mechanisms*

SEVECOM

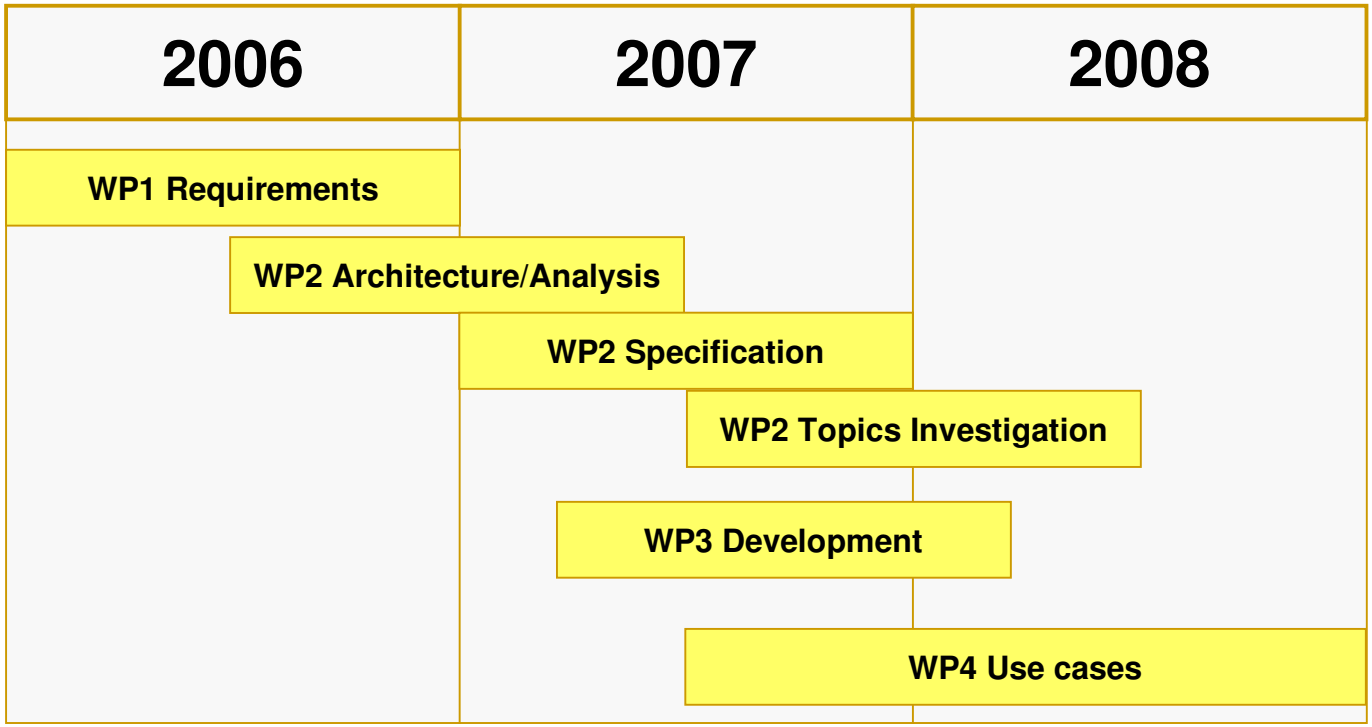
- This task will focus on A1, A2, A3, A6 topics
- Specify the operation of the various security mechanisms taking into account the results of other projects (GST, IEEE P1556, etc.)
- Specify the cryptographic functions needed to support the architecture
- Define the interfaces necessary for maintaining compatibility with other systems and integration into the infrastructure
- Prepare the resulting specifications for potential standardization efforts

WP2 – Task 4: *Investigation of Specific Topics*

SEVECOM

- This task will focus on:
  - Intrusion detection (A4)
  - Data consistency (A5)
  - Secure positioning (A7)
  - Secure user interface (A8)
- Investigate the related issues
- Identify research and development gaps
- Propose a roadmap for future work

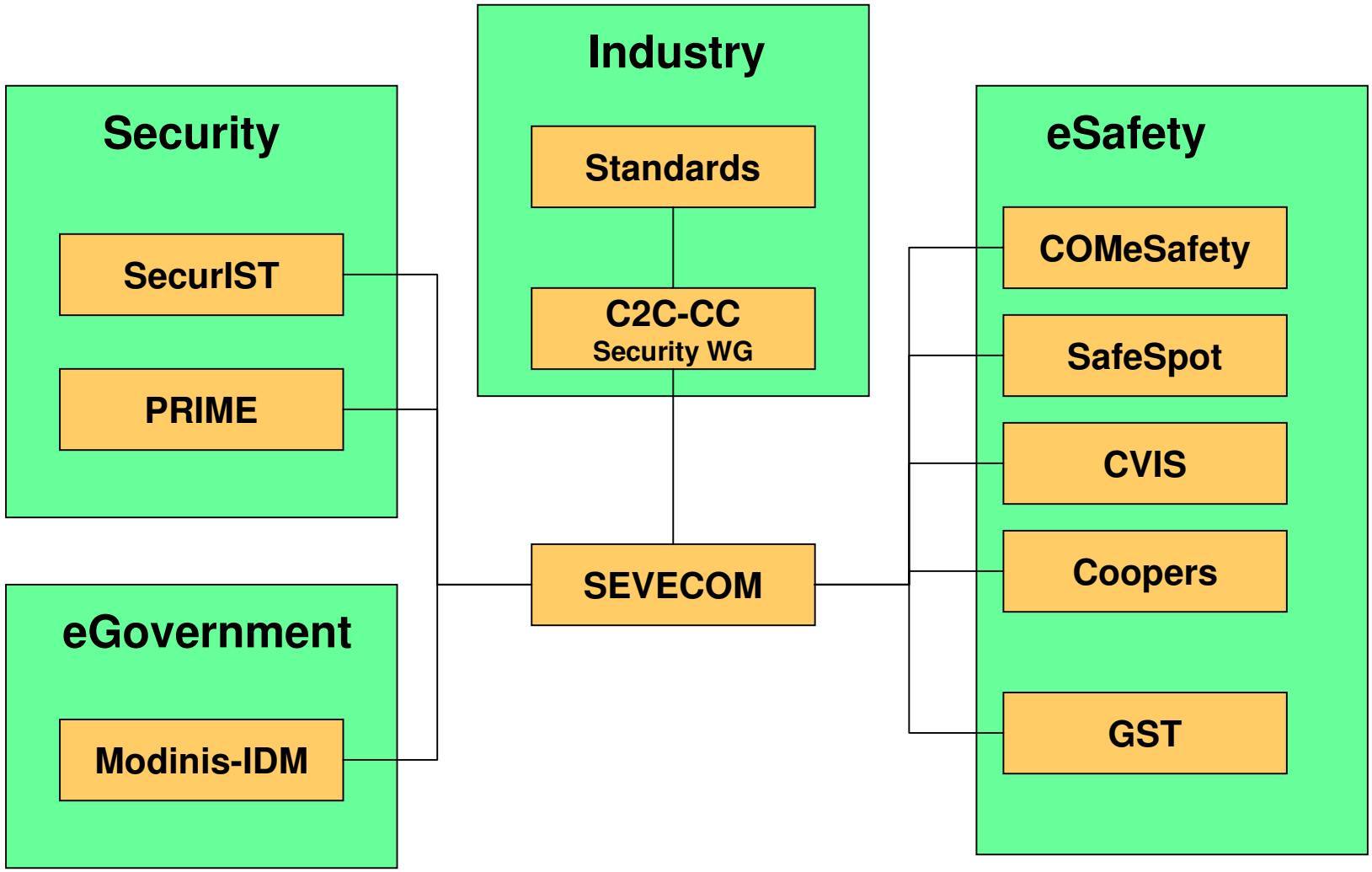
Timetable


2006
2007
2008
WP1 Requirements
WP2 Architecture/Analysis
WP2 Specification
WP2 Topics Investigation
WP3 Development
WP4 Use cases

Liaison: SEVECOM Starting Points

- Trust
  - Contribution from GST-SEC on secure communication
- Privacy and Identity Management
  - Prime generic architecture
  - IDM-Modinis terminology
    - https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc
  - IDM-Modinis conceptual framework

SEVECOM is a Transversal Project



SEVECOM Impact

- V2I/V2C architectures are impacted by privacy and identity management approaches
- Liaison with eSafety projects working on architecture is key
  - Sevecom workshop, Lausanne, 1-2 February 2006
    - Sevecom, CVIS, Safespot, Coopers, COMeSafety, Now, C2C-CC
  - Joint workshop, Lämmerbuckel, 11-12 April 2006
    - Sevecom, CVIS, Safespot, COMeSafety
  - Sevecom workshop, Paris, 26-27 June 2006
    - Sevecom, C2C-CC
  - Joint workshop, Budapest, 4-5 September 2006
    - Sevecom, CVIS, Safespot, Coopers, COMeSafety, C2C, Prime
  - Joint-C2C workshop, Berlin, 15-16 November 2006
    - Sevecom, C2C-CC

Thank you for your attention