Sevecom

Secure Vehicle Communication

Secure Vehicular Communications Workshop Lausanne. February 1st/2nd 2006 Hosted by EFPL

Antonio Kung

SEVECOM Project Co-ordinator

TRIALOG

Workshop Organised by SEVECOM

- SE-cure VE-hicle COM-munication
- 3-year European Project 2006-2007-2008

Information Society and Media

Safety

- Partners
  - Trialog (Coordinator)
  - DaimlerChrysler
  - Centro Riserche Fiat
  - Philips
  - Ecole Polytechnique Fédéral de Lausanne
  - University of Ulm
  - Budapest University of Technology and Economics

eSafety Projects

- Current projects include

AIDE	EASIS	PReVENT	Advanced Protective Systems	GST: On-line Safety Services
Adaptive Integrated Driver-vehicle Interface -Driver Modelling -HMI Design -Evaluation	Electronic Architecture and System Engineering for Integrated Safety Systems	Integrated Preventive Safety Systems: -Lane Keeping -Collision Warning -Intersect. Control - ...	Enhanced restrain and protection systems. Crashworthiness	Traffic Info. Hazard Warning Rescue Service
BMW, CRF, DC, Ford, Opel, Seat Renault, PSA	CRF, DAF Opel, PSA, Renault, Volvo	BMW, CRF, Ford, Opel, Renault, PSA, VW, Volvo	DC, PSA, Renault, VW	BMW, DC, Opel, CRF Renauld,Ford
Volvo	**DC**	**DC**	**TNO**	**Ertico**

  - Part of the EUCAR Program for Integrated Safety
- New projects to be started in 2006 include
  - SafeSpot, CVIS, Coopers : Applications on V2V & V2I
  - SEVECOM: Security of V2V & V2I
  - COMeSafety: coordinating V2V and V2I related projects

SEVECOM

- Mission: define a consistent and future-proof solution to the problem of V2V/V2I security
- Focus: communications specific to road traffic. Includes messages related to
  - traffic information,
  - anonymous safety-related messages,
  - liability-related messages
- Approach: close collaboration with eSafety project and with the C2C consortium

SEVECOM Objectives

- Architecture and security mechanisms
  - provides the right level of protection.
  - addresses issues such as liability versus privacy
- Fully addressed topics
  - Key and identity management,
  - Secure communication protocols (including secure routing),
  - Tamper proof device and decision on crypto-system,
  - Privacy.
- Investigated topics
  - Intrusion Detection,
  - Data consistency,
  - Secure positioning,
  - Secure user interface.

SEVECOM Objectives

- Cryptographic primitives which take into account the specific operational environment
  - These primitives will be adaptations of existing cryptosystems to the VC environment.
- Challenges is to address
  - the variety of threats,
  - the sporadic connectivity created by moving vehicles and the resulting real-time constraints,
  - the low-cost requirements of embedded systems in vehicles.

Milestones

Semester 2: M1

- Requirements
- Initial architecture

Semester 3: M2

- Final architecture
- Initial security mechanisms specification
- Approaches for specification validation

Semester 4: M3

- Final security mechanisms specification
- Initial developments
- First results on *investigated topics*
- Security specification validation
- Approaches for implementation validation
- Roadmap v1

Semester 5: M4

- Validated developments
- Final results on *investigated topics*

Semester 6: M5

- Use case implementation
- Validation through use case
- Roadmap v2

Workshop Programme

Wednesday, February 1, 2006

- Opening Session
  - 08.30 A.Kung Opening talk
  - 08.45 M.Provera. The SafeSpot Project
  - 08.50 M.Nemec. The Coopers Project
  - 09.00 K.Evensen. The CVIS Project
- Session 1: Standards, Platforms, Tools
  - 09.10 K.Evensen. The CALM architecture and security issues
  - 09.40 R.Kroh. Vehicle Standards and In-Vehicle Protection Issues
- 10.20 Break
  - 10.50 A.Kung. Secure Execution Environment for V2V and V2I Communication
  - 11.20 F.Kargl. Vanet simulations with JIST/SWANS
  - 12.00 Lunch
- Session 2: Tamper-Proof Devices
  - 13.00 L.Buttyan. Tamper-Resistant Devices
  - 13.40 R.Mietzner. ComeSafety
  - 14.20 Break
- Session 3: Key and Identity Management
  - 14.50 M.Gerlach. On identification and addressing
  - 15.20 M.Raya. Key Management for Vehicular Networks
- 16.00 Break
- Session 4: Privacy
  - 16.30 J.Camenisch. Privacy-Protecting Authentication
  - 17.30 M.Gerlatch. Privacy in the Network on Wheels project
- 18.00 Closing remarks
- 19.30 Dinner

Thursday, February 2, 2006

- Session 5: Secure communication
  - 09.00 F.Kargl. Secure Routing for Vehicular Networks
  - 09.30 T.Leinmueller. Security and Geographic Routing
- Session 6: Intrusion Detection
  - 10.00. T.Leinmueller. Concepts for a V2x Intrusion detection System
- 10.30 Coffee break
- Session 7: Open-floor discussion
  - 11.00 Discussion
- 12.00 Closing remarks
- 12.15 Lunch

Sevecom

Secure Vehicle Communication

Thanks!

And thanks to EPFL for Hosting this event