

## LABORATORY FOR COMMUNICATIONS AND APPLICATIONS LCA

### Security of Vehicular Network



### What are Vehicular Networks?

Vehicular Networks (also known as VANETs) are a cornerstone of the envisioned Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC), vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities. The interesting research area of Vehicular Networks is where ad hoc networks can be brought to their full potential.

### Security of Vehicular Networks

To become a real technology that can guarantee public safety on the roads, vehicular networks need an appropriate security architecture that will protect them from different types of security attacks. Leveraging on the expertise of LCA in the domains of networking and security, we are exploring the different security aspects of vehicular networks, including:

- Threat model
- Authentication and key management
- Privacy
- Secure positioning

### Publications

#### Security Requirements and Architecture

P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, **Secure vehicular communications: design and architecture**, IEEE Communications Magazine, vol. 46, no. 11, pp. 100-109, November 2008 [pdf]

F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, J.-P. Hubaux, **Secure vehicular communication systems: implementation, performance, and research**

**challenges**, IEEE Communications Magazine, vol. 46, no. 11, pp. 110-118, November 2008 [pdf]

P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, **Architecture for Secure and Private Vehicular Communications**, In Proceedings of the 7th International Conference on ITS Telecommunications, June 2007 [pdf]

P. Papadimitratos, V. Gligor, and J.-P. Hubaux. **Securing Vehicular Communications - Assumptions, Requirements, and Principles**, In Proceedings of the Workshop on Embedded Security in Cars (ESCAR) 2006, November 2006. [pdf]

M. Raya, P. Papadimitratos, and J.-P. Hubaux, **Securing Vehicular Communications**, In IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, October 2006 [pdf]

M. Raya and J.-P. Hubaux, **The Security of Vehicular Ad Hoc Networks**, In Proceedings of SASN 2005, November 2005 [pdf]

M. Raya and J.-P. Hubaux, **Security Aspects of Inter-Vehicle Communications**, In Proceedings of STRC 2005 (Swiss Transport Research Conference), March 2005 [pdf]

J.-P. Hubaux, S. Capkun and J. Luo, **The Security and Privacy of Smart Vehicles**, IEEE Security & Privacy Magazine, Vol. 2, No. 3, pp 49--55, May-June 2004 [pdf]

J. Luo and J.-P. Hubaux, **A Survey of Inter-Vehicle Communication**, EPFL Technical Report IC/2004/24, March 2004 [pdf]

## Trust and Revocation

M. Raya, M. H. Manshaei, M. Felegyhazi, and J.-P. Hubaux, **Revocation Games in Ephemeral Networks**, Proceedings of ACM CCS 2008, October 2008 [pdf]

M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, **On Data-Centric Trust Establishment in Ephemeral Ad Hoc Networks**, Proceedings of INFOCOM 2008, April 2008 [pdf]

M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, **Eviction of Misbehaving and Faulty Nodes in Vehicular Networks**, IEEE Journal on Selected Areas in Communications, Special Issue on Vehicular Networks, 2007 [pdf]

## Authentication

G. Calandriello, P. Papadimitratos, A. Lloy, and J.-P. Hubaux, **Efficient and Robust Pseudonymous Authentication in VANET**, In Proceedings of VANET 2007, September 2007 [pdf]

M. Raya and J.-P. Hubaux, **Securing Vehicular Ad Hoc Networks**, Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, Vol. 15, Nr. 1, pp. 39 - 68, 2007 [pdf]

## Privacy

J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, and J.-P. Hubaux, **Mix-Zones for Location Privacy in Vehicular Networks**, In Proceedings of WiN-ITS, August 2007 [pdf]

E. Schoch, F. Kargl, T. Leinmuller, S. Schlott, and P. Papadimitratos, **Impact of Pseudonym Changes on Geographic Routing in VANETs**, In Proceedings of the European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS), October 2006. [pdf]

P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl, **Privacy and Identity Management for Vehicular Communication Systems: A Position Paper**, Workshop on Standards for Privacy in User-Centric Identity Management,

Zurich, Switzerland, July 2006. [pdf]

## Miscellaneous

C. Harsch, A. Festag, and P. Papadimitratos, **Secure Position-Based Routing for VANETs**, To appear in Proceedings of the IEEE VTC2007-Fall, October 2007 [pdf]

M. Raya, A. Aziz, and J.-P. Hubaux, **Efficient secure aggregation in VANETs**, In *Proceedings of VANET 2006*, September 2006 [pdf]

T. Leinmueller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, **SEVECOM - Secure Vehicle Communication**, IST Mobile and Wireless Communication Summit, Mykonos, Greece, June 2006.

## Presentations and Posters

M. Raya, P. Papadimitratos, and J.-P. Hubaux, **Securing Vehicular Networks**, Slide show [ppt]

M. Raya, P. Papadimitratos, and J.-P. Hubaux, **Securing Vehicular Networks**, In Infocom'06 - Poster session, April 2006 [pdf]

## Simulation of VANETs

We have completed a new, realistic, and open-source simulation environment for VANETs called TraNS. Follow this link for more information: <http://trans.epfl.ch>.

## EVENTS

---

AutoNet

escar

Int. Work. Veh. Comm.

LCN ON-MOVE

MOVE

VANET

VTC

V2VCOM

Vehi-Mobi

WIT

WiVeC

## PEOPLE

---

Prof. Jean-Pierre Hubaux

Dr. Panos Papadimitratos

Maxim Raya

Julien Freudiger

Collaborators

Prof. Levente Buttyan  
Prof. Srdjan Capkun  
Dr. Frank Kargl

## **RELATED**

---

At EPFL

SmartPark

TraNS

MICS

Projects

Car2Car

California PATH

eSafety

NOW

SeVeCom