KTH Electrical Engineering

Privacy-preserving PKI for Location-based Services

Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos

Networked Systems Security Group
Royal Institute of Technology, Stockholm, Sweden

Abstract

Location-based services (LBS) and pay-as-you-drive systems are expected to grow in popularity, also thanks to the upcoming vehicular communication (VC) systems. Such emerging applications are posing new challenges for existing Vehicular Public Key Infrastructure (VPKI) architectures; notably, support for Authentication, Authorization and Accountability (AAA), without exposing vehicle privacy. At the same time, mobile users in general, not only users of VC systems, are increasingly sensitive to reduce exposure of user profile while fully benefiting from LBS. The goal is to secure user-to-user and user-to-system interactions while preserving anonymity and unlinkability. Our work and the solutions shown here cater exactly to this need: we enable AAA services while reducing the user exposure.

Our Contribution for Key Management

- Privacy-preserving identification and credential management infrastructure
- Use of cryptographic tickets to support AAA
- Conditional anonymity through the use of pseudonyms
- Unlinkability between users' long-term identities and provided pseudonyms, and among pseudonyms themselves
- Introduction of multiple LTCAs (Long-Term CA) & PCAs (Pseudonym CA) for reducing the threat of collusion among infrastructure entities
- Provision of location-based services conditionally anonymous & transparent to the LBS

Our Contribution to LBS Privacy

- Unlinkability among LBS queries, users' location and identity (tracing of users)
- Submission of user information in a privacy-preserving manner; no real identity is exposed to the LBS server
- No trusted third-party server is required (e.g., no trust to LBS server, MobiCrowd [3])

Basic Goals

- Support for a gamut of communication modes; V2V (Vehicle-2-Vehicle), V2I (Vehicle-2-Infrastructure) and V2M (Vehicle-2-Mobile), and M2M (Mobile-2-Mobile)
- Provision of comprehensive security & privacy mechanisms for reducing users' personal information leakage

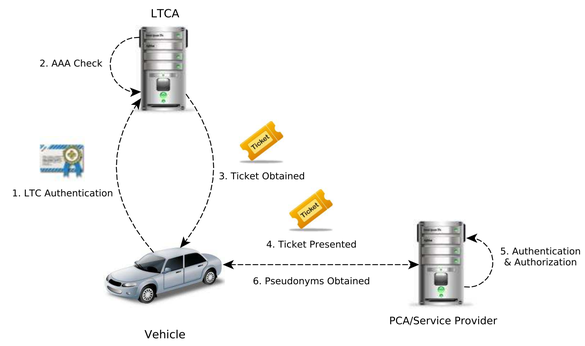
Basic Components in the Demo

- Two laptops, representing the LTCA & the PCA
- Smart-phones communicating with the LTCA and the PCA to obtain tickets and pseudonyms

Sequence of Demonstration

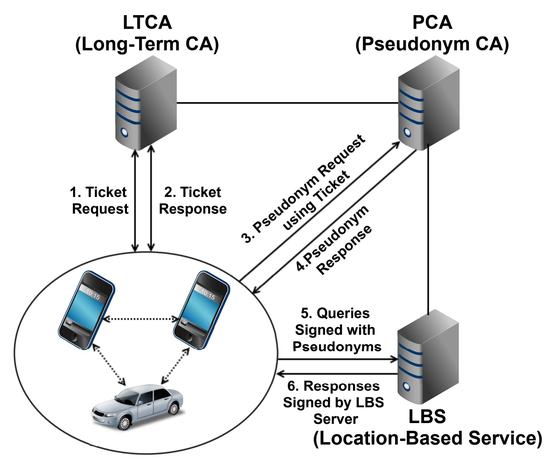
- LBS queries are generated & signed by users using pseudonyms, provided by VeSPA
- Multicast LBS queries among registered smart-phones
- Communication with the LBS server *directly* if not enough Point-of-Interests (POIs) are received by peers

VeSPA: Vehicular Security and Privacy-preserving Architecture



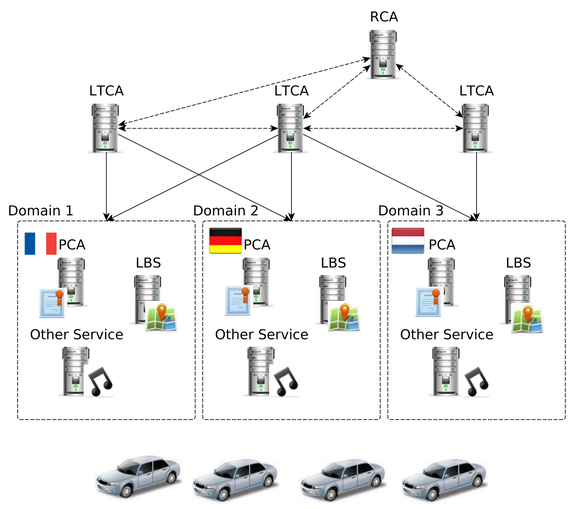
- Efficient VPKI (Vehicular Public Key Infrastructure) credential management architecture
- Scalable privacy-preserving VPKI
- Use of cryptographic **tickets** to support AAA; Kerberized-tickets facilitate access control across multiple domains
- Conditional anonymity
- Compliance with IEEE 1609.2

Client Interaction with VeSPA and LBS Servers

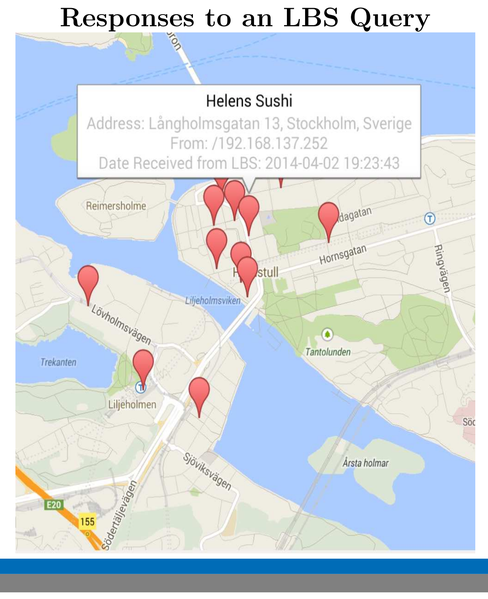


- Fully *cross-platform* system, accessible via any device
- Credentials allow anonymous data submission and/or querying
- Service discovery in an efficient way (i.e., low latency) while protecting users' privacy

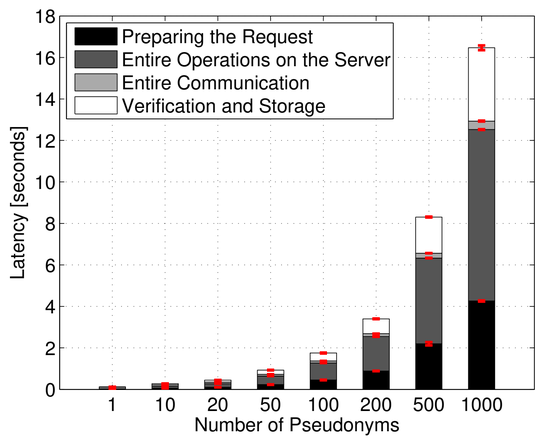
VeSPA Multi-Domain and Multi-Service Architecture



Responses to an LBS Query



VeSPA Scalability



Latency to obtain pseudonyms per client

Summary

- Comprehensive identity and service management
- Privacy-preserving access to location-based services
- Full-blown implementation for different settings and platforms
- Scalable design
- More efficient next version of VeSPA (in testing)

References

[1] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos. **"VeSPA: vehicular security and privacy-preserving architecture"**. In Proceedings of the 2nd ACM Workshop on Hot Topics on Wireless Network Security and Privacy (ACM HotWisec). Budapest, Apr. 2013.

[2] V. Manolopoulos, P. Papadimitratos, S. Tao, and A. Rusu, **"Securing Smartphone Based ITS"**. in Proceedings of the 11th IEEE International Conference in ITS Telecommunications (IEEE ITST), St.Petersburg, Russia, September 2011.

[3] R. Shokri, P. Papadimitratos, and J.-P. Hubaux, **"MobiCrowd: A Collaborative Location Privacy Preserving LBS Mobile Proxy"**. In Proceedings of the ACM International Conference on Mobile Systems, Applications and Services (ACM MobiSys), San Francisco, CA, USA, June 2010.