PRECIOSA PeRA: Practical Enforcement of Privacy Policies in Intelligent Transportation Systems

[Extended Abstract]

Martin Kost
DBIS Group
Humboldt University
Berlin, Germany
kost@informatik.hu-berlin.de

Björn Wiedersheim
Institute of Media Informatics
Ulm University, Germany
bjoern.wiedersheim@uni-ulm.de

Stefan Dietzel
DIES Group
University of Twente
Enschede, The Netherlands
s.dietzel@utwente.nl

Florian Schaub
Institute of Media Informatics
Ulm University, Germany
florian.schaub@uni-ulm.de

Tobias Bachmor
Planung Transport Verkehr AG
Karlsruhe, Germany
tobias.bachmor@ptv.de

ABSTRACT

Cooperative Intelligent Transportation Systems must incorporate privacy enhancing mechanisms to gain acceptance by all involved parties. The PRECIOSA Privacy-enforcing Runtime Architecture (PeRA) provides a holistic privacy protection approach, which implements user-defined privacy policies. A data-centric protection chain ensures that ITS components process data according to attached privacy policies. PeRA instances constitute a distributed privacy middleware, which evaluates privacy policies to mediate data access by applications. The architecture includes an integrity protection layer to create a distributed policy enforcement perimeter between ITS nodes, which prevents the circumvention of policies. The PeRA has been implemented in a proof-of-concept prototype.

1. INTRODUCTION

Future Intelligent Transportation Systems (ITS) consist of vehicles, roadside units, access networks, and backend services. These ITS nodes exchange information with each other in order to provide improved functionalities such as enhanced travel services, driving support, and transportation optimization. Such services impact the privacy of individuals (e.g., vehicle owners and drivers) due to required location information and related personal information. Uncontrolled information flows constitute the potential for privacy infringements (e.g., generation of driving/movement profiles). The issue of privacy protection has been recognized by jurisdiction on a European level [4, 5]. We argue that technological means must complement legislation.

Most technical proposals for privacy preservation in ITS focus on single applications, like road tolling [2, 3] or pay-as-you-drive insurance [8, 9]. In the PRECIOSA project [1], we took a different approach, developing a policy-based privacy enforcement architecture, which provides an application independent privacy middleware for ITS.

2. PRECIOSA PERA

The PRECIOSA Privacy-enforcing Runtime Architecture (PeRA) implements a data-centric approach for privacy protection (cf. Fig. 1). All data is combined with an immutable privacy policy upon creation, which is defined by the data owners/subjects. Mandatory privacy control (MPC) components ensure that applications can only perform policy compliant operations on the data. To prevent data processors from circumventing the MPC we introduce the MPC integrity protection (MIP) layer. The MIP layer stores data securely and encrypts data for information exchange between PeRA instances. The MIP monitors the integrity of MPC components and only grants data access if all MPC components are in a trusted state.

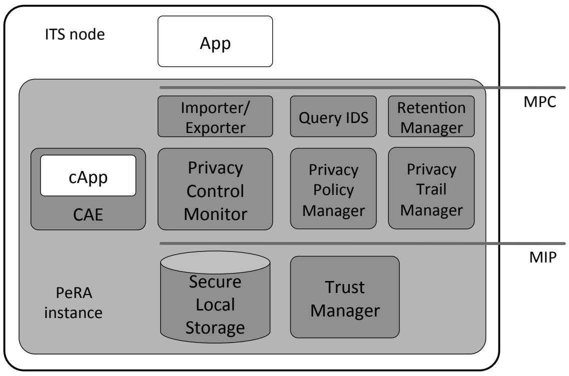

Figure 1: Overview of the PRECIOSA PeRA.

2.1 Mandatory Privacy Control

The MPC components mediate all data access and processing. An application poses an operation request as a query to the Privacy Control Monitor (PCM). The PCM evaluates the privacy policies of affected data items. Based on the evaluation result, a query is rejected or executed. Also, the MPC may perform additional data transformations on the data to meet the privacy requirements specified in attached policies. For instance, the MPC may perturb a result set to reach a certain anonymity set size or obfuscate location data.

We guarantee for all data that leaves the PCM to be policy compliant. However, once outside the control of the PeRA, we cannot guarantee policy enforcement anymore. Therefore, external applications may not gain data access on the required level of detail. Thus, we integrated an application sandbox, the Controlled Application Environment (CAE). Application parts running inside the CAE are heavily restricted in their communication and resource access capabilities. But controlled applications may have detailed data access, which is mediated and controlled by CAE and PCM.

Additional MPC components ensure policy-compliant data retention, provide verifiability with a privacy trail, and monitor queries for probing and correlation attacks.

2.2 MPC Integrity Protection

The Trust Manager is the main component of the MIP layer and has two major tasks. (1) All data of a PeRA instance is stored inside an encrypted storage repository. The Trust Manager ensures that the interface of the secure repository is only exposed to the PCM. (2) The Trust Manager monitors the integrity of the MPC components. Reference integrity measurements are stored inside a hardware security module (HSM), serving as a hardware trust anchor. The HSM also holds the key material of a PeRA instance, i.e., keys for storage encryption and for confidential communication with other PeRA instances. As soon as the Trust Manager detects an integrity violation of any MPC component the HSM blocks key usage, and therefore access to stored data. We developed a non-interactive remote attestation protocol [6] to accommodate the special communication requirements of ITS.

3. EXAMPLE: FCD

We use a Floating Car Data (FCD) use case to demonstrate how privacy-preserving ITS applications can be realized by using the PeRA. Multiple vehicle nodes submit FCD records to a backend server. FCD records contain information about the vehicle's current location, speed, and traffic density. In a vehicle node, an application running in the CAE requests to send of sensor information, including position and speed. The local PCM evaluates the request, fetches the sensor information, and attaches a user-defined privacy policy to the FCD record. The Exporter encrypts the FCD record in cooperation with the Trust Manager and configures the communication subsystem for pseudonym use [7]. On the server node, the Importer decrypts the information together with the Trust Manager. The data is then imported into a secure local storage. Different applications request to process data, which is granted in compliance with the attached privacy policies. We exemplify two scenarios. (1) A traffic information system that can only receive aggregated and anonymized information, and (2) a freight tracking system that is able to access location samples of commercial trucks.

4. PERA PROTOTYPE

To demonstrate feasibility, we created a proof-of-concept PeRA implementation based on OSGi. PeRA components and applications are implemented as OSGi bundles. We use the Java/OSGi security system to control and restrict access rights of OSGi bundles. Thus, it is ensured that only the PCM can access the secure repository. The PeRA components are shielded from applications by only exposing dedicated query interfaces. Integrity protection is realized in two phases: bundle signature verification on load and dynamic monitoring by the Trust Manager at runtime. A Trusted Platform Module (TPM) is employed as a low-cost HSM.

5. CONCLUSIONS

The PeRA constitutes a holistic approach to protect privacy in ITS. Online policy evaluation provides the necessary flexibility to accommodate individual privacy preferences of all stakeholders. PeRA is a privacy middleware that ensures privacy policy compliant data processing throughout an Intelligent Transportation System. With our proof-of-concept implementation we show the viability of the proposed concepts. Further refinement and evaluation is required to ensure that scalability requirements of future ITS can be met. Also, engagement in public policy and legislation debates is necessary to successfully integrate technical privacy solutions in the ITS ecosystem.

6. REFERENCES

[1] Preciosa (privacy enabled capability in co-operative systems and safety applications) FP7 project. Online www.preciosa-project.org.

[2] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, and C. Geuens. PrETP: Privacy-preserving electronic toll pricing. In *USENIX*, pages 63–78, 2010.

[3] A. Cavoukian. 407 express toll route: How you can travel the 407 anonymously. Online, May 1998. Information and Privacy Commissioner Ontario.

[4] European Parliament and Council. Directive 2010/40/EU. Official Journal L 207, 06/08/2010 P. 1–13, July 2010.

[5] P. Hustinx. EDPS opinion on intelligent transport systems. *Opinions of the EU Data Protection Supervisor*, July 2009.

[6] F. Kargl, F. Schaub, and S. Dietzel. Mandatory Enforcement of Privacy Policies using Trusted Computing Principles. In *Proc. Intelligent Information Privacy Management, AAAI Spring Symposium*, Stanford University, 2010. AAAI.

[7] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communications: Design and architecture. *IEEE Communications Magazine*, 46(11):100–109, Nov. 2008.

[8] R. A. Popa, H. Balakrishnan, and A. Blumberg. VPriv: Protecting Privacy in Location-Based Vehicular Services. In *USENIX Security Symposium*, 2009.

[9] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel. Pripayd: privacy friendly pay-as-you-drive insurance. In *Proc. workshop on Privacy in electronic society*, pages 99–107. ACM, 2007.