WiSec 2011 Demo: PRECIOSA PeRA – Practical Enforcement of Privacy Policies in Intelligent Transportation Systems

Martin Kost[a] *kost@informatik.hu-berlin.de*
Björn Wiedersheim[b] *bjoern.wiedersheim@uni-ulm.de*
Stefan Dietzel[c] *s.dietzel@utwente.nl*
Florian Schaub[b] *florian.schaub@uni-ulm.de*
Tobias Bachmor[d] *tobias.bachmor@ptv.de*
[a]DBIS Group, Humboldt University, Berlin, Germany
[b]Institute of Media Informatics, Ulm University, Ulm, Germany
[c]DIES Group, University of Twente, Enschede, The Netherlands
[d]Planung Transport Verkehr AG, Karlsruhe, Germany

Cooperative Intelligent Transportation Systems must incorporate privacy-enhancing mechanisms to gain public acceptance. The PRECIOSA Privacy-enforcing Runtime Architecture (PeRA) provides a data-centric protection chain, which ensures that ITS components process data according to attached user-defined privacy policies. PeRA instances constitute a distributed privacy middleware that evaluates privacy policies to mediate data access by applications. An integrity protection layer creates a distributed policy enforcement perimeter between ITS nodes to prevent circumvention of policies. The PeRA has been implemented as a proof-of-concept prototype.

I. Introduction

Intelligent Transportation Systems (ITS) consist of vehicles, roadside units, access networks, and backend services. These ITS nodes exchange information to provide enhanced travel services, driving support, or transportation optimization. Such services impact the privacy of individual drivers due to required location and personal information. Uncontrolled information flows constitute potential for privacy infringements, e.g., generation of movement patterns. This privacy issue has been recognized by jurisdiction on a European level [3, 4]. We argue that technological means must complement legislation. Most proposals for privacy protection mechanisms in ITS focus on single applications, like road tolling [2]. 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.

II. PRECIOSA PeRA

The PRECIOSA Privacy-enforcing Runtime Architecture (PeRA) implements a data-centric approach for privacy protection (cf. Fig. 1). Upon creation, all data is combined with an immutable privacy policy defined by users. Mandatory privacy control (MPC) components ensure that applications can only perform policy-compliant operations on data. The MPC integrity protection (MIP) layer prevents data processors from circumventing MPC. The MIP layer handles encrypted storage and encrypted information exchange between PeRA instances. The MIP monitors integrity of MPC components and only grants data access if all MPC components are in a trusted state.

II.A. Mandatory Privacy Control

The MPC components mediate all data access and processing. Applications pose operation requests as queries to the Privacy Control Monitor (PCM). The PCM evaluates privacy policies of affected data items and either rejects or executes a query. Also, the PCM may perform additional data transformations to meet privacy requirements specified in attached policies. For instance, the PCM may perturb a result set to reach a certain anonymity value or obfuscate location data. We guarantee for all data that leaves the PCM to be policy compliant. However, once outside the control of PeRA, policy enforcement cannot be provided 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 restricted in their communication and resource access capabilities by CAE and PCM. These applications get con-

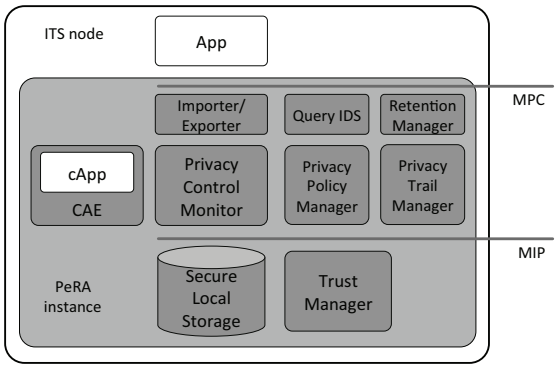

Figure 1: Overview of the PRECIOSA PeRA.

trolled access to the required data. Additional MPC components ensure policy-compliant data retention, keep privacy trails, and monitor queries for probing and correlation attacks.

II.B. MPC Integrity Protection

The Trust Manager is the main component of the MIP layer and provides two major functionalities. (1) All data of a PeRA instance is stored inside an encrypted storage that only the PCM can access. (2) The Trust Manager monitors the integrity of MPC components. A hardware security module (HSM) stores reference integrity measurements and key material, which is used for encrypted storage and confidential communication with other PeRA instances. As soon as we detect an integrity violation of any MPC component the HSM blocks key usage, and thus access to stored data. A non-interactive remote attestation protocol [5] is used to cope with intermittent connectivity in ITS.

II.C. FCD Example and PeRA Prototype

We use a Floating Car Data (FCD) use case to demonstrate how privacy-preserving ITS applications can be realized by using the PeRA. In the use case, vehicles submit FCD records to a backend server. FCD records contain location, speed, and traffic density information. In a vehicle node, a CAE-controlled application requests to send respective sensor information. 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 to use pseudonyms. On the server node, the Importer decrypts the information together with the Trust Manager and imports the data 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 only receiving aggregated/anonymized information, and (2) a freight tracking system accessing location traces of commercial trucks.

To demonstrate feasibility, we created a proof-of-concept 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 at runtime. A Trusted Platform Module (TPM) is employed as a low-cost HSM.

III. Conclusions

The PeRA constitutes a holistic approach to privacy protection in ITS. Online policy evaluation provides the necessary flexibility to accommodate individual privacy preferences. PeRA is a privacy middleware that ensures privacy-policy-compliant data processing. 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.

References

[1] PRECIOSA (PRivacy Enabled Capability In Co-Operative Systems and Safety Applications) FP7 project. `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 Security Symposium*, 2010.

[3] European Parliament and Council. Directive 2010/40/EU. Official Journal L 207, July 2010.

[4] P. Hustinx. EDPS opinion on Intelligent Transport Systems. *Opinions of the EDPS*, July 2009.

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