Privacy-Enhancing Access Control Enforcement

Yves Deswarte Matthieu Roy
LAAS-CNRS*

September 13, 2006

Abstract

In this paper, we show that a clear separation between Access Control Decision and Access Control Enforcement helps in efficiently controlling accesses to sensitive data, which is essential for information security and privacy. This is particularly important when retrieving Personally Identifying Information (PII) from database servers.

1 Introduction

The PRIME architecture implements a separation between Access Control Decision Function (ACDF) and Access Control Enforcement Function (ACEF), which should help to respect the least privilege principle.

The base concept for implementing such a separation is a *composite operation*: when accessing personal information (e.g. a bank transfer), different personal data are to be retrieved and processed in a single transaction. A composite operation is a pattern of accesses that represent a complete transaction. Using this concept, the decision can be taken at a coarse grain level, where the semantics of the request can be used to take the decision, while the enforcement can be done at a fine grain level, (e.g., each elementary access to a PII—Personally Identifying Information), so that only legitimate accesses are granted.

But this separation between ACDF and ACEF raises interesting research problems: how to recognize if a particular access is compliant with a positive decision, i.e., is the access necessary for the execution of an authorized operation, or is the operation execution doing more than what is legitimate? So it is necessary to analyze the consistency between functionality requirements (what accesses are necessary for the execution of the operation), security and

*This work is partially supported by the PRIME project —Privacy and Identity Management for Europe— project IST 507591

privacy objectives (what properties must be guaranteed?), and policy rules (how to decide if an operation is legitimate or not?).

The proposed research aims also to go further than the current PRIME architecture paradigm, which results from some trade-off between efficiency and constraints on the development of PRIME modules and applications: even if PII access is the most important point of access control enforcement, it would be interesting to analyze how more stringent approaches, such as information flow control, could be developed to cope with privacy and identity management requirements. There are many information flow control models, but very few mechanisms have been proposed to enforce them. More research is thus needed on this area.

2 Privacy-enhancing access control

There is no privacy, and identity management is of no use, if the privacy and identity management policy is not enforced. This is particularly important for servers processing personal information, but this is also true on the user side to protect the identity management functions against malicious or erroneous code.

Strong access control enforcement is thus necessary to prevent personal information leakage due to accidental events (software bugs, user or operator mistakes) or malicious actions performed by hackers or disgruntled employees.

2.1 Current status

The first analysis of the relations between access control decision and access control enforcement has led to the definition of the access control module in the current PRIME architecture, with the definition *composite operations*, and the corresponding *authorisation proofs* for interaction between decision and enforcement.

The control flow of a typical transaction, as shown in Figure 1, is the following:

1. the user asks the Access Control Decision Function to grant rights for a *composite operation*.

2. the ACDF, based on security and privacy policies, computes the decision concerning the requested accesses.

3. if the decision is positive, the user is permitted to access data: ACDF sends a decision identifier (DiD) to the user, and generates authorisation proofs that are sent to ACEF (Access Control Enforcement Function).

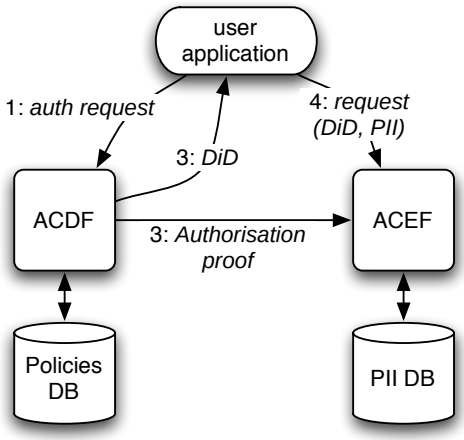

Figure 1: Simplified schema of Access Control in PRIME

4. when the application performs the operations (i.e. accesses PII— Personally Identifying Information), it sends with its requests the provided DiD, and the ACEF can verify if every access is part of the requested transaction, by using the authorisation proof.

A first method to create composite operation templates has been developed, and can be applied on simple examples. These templates are statically defined both for composite operations and for authorisation proofs, and correspond to classical patterns of accesses to PII.

2.2 Current ACEF Research in PRIME

In order to have a more complete solution, we are currently working on improving the above-presented solution in different aspects:

1. Analyze the correspondence between authorization decision and detailed operation execution, both on practical examples (code analysis) and at an abstract level (specification and development of application modules).

2. Develop methods and tools to create templates of operation executions, necessary for the automatic generation of authorization proofs (the authorization proofs are generated when an ACDF decision is positive, and checked by the ACEF for each access to a PII). The creation of templates can be done manually or possibly automatically through code analysis, but it is desirable to create them at a more abstract level, since this could help to verify (possibly formally) the consistency of the execution requirements (abstracted in the template) with the privacy and security objectives and the policy rules. Research is needed for that, since no state-of-the-art techniques exist so far.

3. Experiment these methods and tools on realistic examples, such as the PRIME applications prototypes.

4. Analyze approaches and techniques to strengthen enforcement mechanisms, by using access control mechanisms provided by open-source operating systems, possibly by improving them with hardware support (X86 rings, TPM, smartcards,). If new promising solutions are discovered, implement and experiment them in a prototype.

5. Analyze approaches and techniques to complement the enforcement mechanisms in protecting PII, in particular against privileged users. At least three approaches are proposed by PRIME partners: cryptography-based sticky policies attached to PII (approach developed by HP Labs); policy-based cryptography (approach developed at Eurecom); fragmentation and scattering of sensitive information (approach developed by LAAS-CNRS).

6. Analyze how information flow models, which have been developed mostly for confidentiality in the defence domain and integrity in the financial domain, can apply to privacy and identity management. For example, in the lattice model, levels should probably correspond more to trust than to confidentiality or integrity classification, while compartments could be corresponding to persons, or groups of persons. For other models, e.g. non-interference or causality, the same adaptation to privacy has to be analyzed, and dedicated mechanisms have to be invented to intercept and control information flows. The implementation of these mechanisms would impact the architecture, of course.

3 Conclusion

In this document, we briefly described the PRIME architecture for controlling accesses to personal identity information. This architecture separates two functions: the decision function and the enforcement. The separation permits to improve access control efficiency, by allowing a series of operations to be part of a single *composite operation* with a more precise semantics. We described a way to link decision and enforcement, by using authorisation proofs, that help in ensuring consistency between decision and enforcement.

In order to have a complete privacy-preserving solution, more research is needed, in particular in the generation of the above-mentioned authorisation proofs, and in the strengthening of enforcement mechanisms.

References

[ABO03] A. Abou El Kalam & R. el Baïda & P. Balbiani & S. Benferhat & F. Cuppens & Y. Deswarte & A. Miège & C. Saurel & G. Trouessin, *Organization Based Access Control*, Proc. 4th IEEE Workshop on Policies for Distributed Systems and Networks (POLICY-2003): pp 120–131, june 2003

[CAS03] M. Casassa Mont & S. Pearson & P. Bramhall, *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*, HP Laboratories Bristol Report HPL-2003-49, 2003

[DES02] Y. Deswarte & N. Abghour & V. Nicomette & D. Powell, *An Intrusion-Tolerant Authorization Scheme for Internet Applications*, Sup. of the Proceedings of the 2002 IEEE-IFIP International Conference on Dependable Systems and Networks (DSN2002) pp. C-1.1 C-1.6, june 2002

[DES06] Y. Deswarte & C. Aguilar Melchor & V. Nicomette & M. Roy, *Protection de la vie privée sur Internet*, Revue de l'Électricité et de l'Électronique (REE), oct 2006

[DES06a] Y. Deswarte & C. Aguilar Melchor, *Current and future privacy enhancing technologies for the Internet*, Annals of Telecommunications / Annales des Télécommunications, Volume 61(3-4): p. 399-417 (apr. 2006)

[NIC97] V. Nicomette & Y. Deswarte, *An Authorization Scheme for Distributed Object Systems*, Proceedings of the 1997 IEEE Symposium on Security and Privacy - Oakland (USA):pp 21–30, May 1997

[FAB94] J-C. Fabre & Y. Deswarte & B. Randell, *Designing Secure and Reliable Applications using Fragmentation-Redundancy-Scattering: An Object-Oriented Approach*, EDCC 1994, pp 21-38