A Formal Framework for Systematic Privacy by Design

Thibaud Antignac
Privatics, CITI lab — Inria
PhD day 2014

Privacy by Design
Formal Methods
Software Engineering

Introduction

Context

Services provided to consumers are more and more personalized. Though it adds incomparable value in some situations, it may endanger privacy if not properly executed.

Indeed, such services heavily rely on personal data. Their management is known to be a delicate issue: a simple privacy policy is not enough. Privacy by Design is an attempt at bringing a new vision on the problem. It can be explained in a very few words: prevention is better than cure.

Problem

A lot of research about Privacy Enhancing Techniques has been done, especially in cryptography and protocols. This results in many blocks often based on crypto-primitives to securely compute, store or communicate data.

However, no systematic method to design architectures nor to formally verify their conformance to a specification has been proposed. As a consequence, privacy-friendly architectures proposed in the literature tend to be ad-hoc and very specialized to the domain considered.

An epistemic framework to reason about architecture properties

We need to express the states of the actors participating to a service. These epistemic states are denoted by using the operators K_i and X_i and are derived from the properties of the architecture through the inference rules.

The difference between K_i and X_i is K_i denotes a logically omniscient knowledge whereas X_i expresses a knowledge bounded to what can be inferred through the inference system. So X_i cannot inverse one-way function such as those at the foundation of cryptographic primitives.

$$\begin{aligned}\phi &::= \phi_0 \mid \neg\phi \\ &\mid \phi_1 \wedge \phi_2 \\ &\mid K_i\ \phi \\ &\mid X_i\ \phi\end{aligned}$$

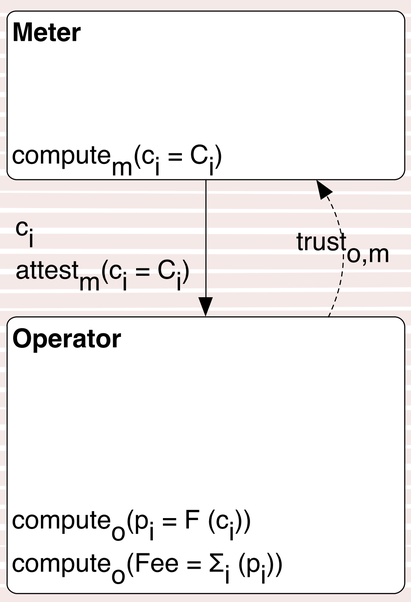
MP: From ϕ and $\phi \rightarrow \psi$ infer ψ
N: From ϕ infer $K_i(\phi)$
K: $K_i(\phi \rightarrow \psi) \rightarrow (K_i(\phi) \rightarrow K_i(\psi))$
KT: $K_i(\phi) \rightarrow \phi$
XT: $X_i(\phi) \rightarrow \phi$
X: From $X_i(\phi_1), \ldots, X_i(\phi_n)$, and $\phi_1, \ldots, \phi_n \rhd_i \phi$ infer $X_i(\phi)$

$$\begin{aligned}\phi_0 &::= receive_{i,j}(x) \mid receive_{i,j}(prim) \\ &\mid trust_{i,j} \\ &\mid compute_i(x = t) \\ &\mid check_i(eq) \\ &\mid has_i(x) \\ &\mid prim \mid p \mid \phi_{01} \wedge \phi_{02} \\ prim &::= proof(p) \mid att \mid prim_1 \wedge prim_2 \\ p &::= att \mid eq \mid p_1 \wedge p_2 \\ att &::= attest_i(eq) \\ eq &::= t_1\ rel\ t_2 \\ rel &::= = \mid < \mid > \mid \leq \mid \geq \\ t &::= d \mid x \mid F(t_1, \ldots, t_n)\end{aligned}$$

$$\begin{aligned}&receive_{i,j}(prim) \rhd_i prim \\ &attest_j(eq), trust_{i,j} \rhd_i eq \\ &proof(p) \rhd_i p \\ &check_i(eq) \rhd_i eq \\ &compute_i(x = t) \rhd_i x = t \\ &hash(x_1) = hash(x_2) \rhd_i x_1 = x_2 \\ &hhash(x) = hhash(x_1) \otimes hhash(x_2) \\ &\qquad \rhd_i x_1 = x_2 \\ &receive_{i,j}(x) \rhd_i has_i(x) \\ &compute_i(x = t) \rhd_i has_i(x) \\ &has_i(x_1), \ldots, has_i(x_n), \\ &\qquad x = F(x_1, \ldots, x_n) \rhd_i has_i(x)\end{aligned}$$

Case study: how to bill smart-metered consumers?

Privacy-intrusive architecture



Specification

The specification generally expresses conflicting requirements between the parties, as it is the case here for the consumption of C_i.

The operator wants:
- $has_o(Fee)$
- $X_o(Fee \geq \Sigma_i(F(C_i)))$

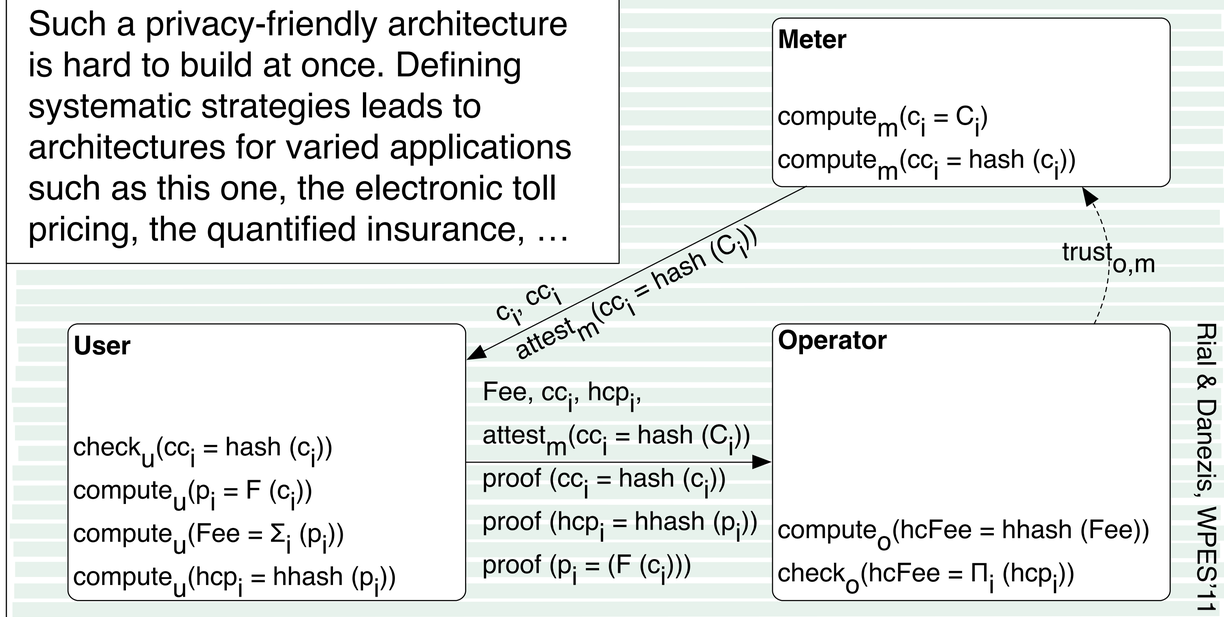
The user wants:
- $\forall i. \neg has_o(C_i)$
- $X_u(Fee \leq \Sigma_i(F(C_i)))$

Two implementations are proposed, the one on the left does not meet the requirements.

Strategies

Such a privacy-friendly architecture is hard to build at once. Defining systematic strategies leads to architectures for varied applications such as this one, the electronic toll pricing, the quantified insurance, …

Privacy-friendly architecture



Rial & Danezis, WPES'11

Conclusion

Synthesis

Privacy by Design is a promising way to build architectures preserving the privacy of the consumers. Though it is still an art-craft to design such architectures, this work is an attempt to provide a formal methods-based framework and a methodology to help to the emergence of standard industrial practices.

Such possibilities are needed by the industry considering the next changes in the legal regulations planned for the following years.

Perspectives

Despite laying some foundations, the perspectives of this work are manifold. The integration of the theoretical framework into a computer-aided design software to support architectures exploration is another step to complete to provide a useful tool.

Moreover, the enhancement of the resolution strategies will lower the specific expertise needed by a designer to use the tool. Patterns, automatic theorem proving or constraint satisfaction problems pave the way for new results.

Thibaud Antignac & Daniel Le Métayer, *Privacy by Design: from Technologies to Architectures (Position Paper)*, APF'14, Athens (Greece).

This work was partially funded by the Inria Project Lab CAPPRIS (Collaborative Action on the Protection of Privacy Rights in the Information Society).