title

"An abstract framework for expressive erasure policies specification"

authors

Filippo Del Tedesco (Chalmers), David Sands (Chalmers), Sebastian Hunt (City University, London)

abstract

Complex internet-based services often require users to provide sensitive data (bank ID, biometric parameters, ...) to accomplish their results, and for this reason they are supposed to meet strict security properties.

One of such properties is referred as (logic) information erasure: once a system is done with a sensitive data, all it "knows" about that data must be "forgotten".

Defining and understanding the erasure property of a system is a complex task, since it involves quantitative aspects (how much the system is really forgetting) but also conditions which have to hold in order for the removal process to be possible.

Existing frameworks to reason about erasure support simple policies specification. Existing implementations deal with more complex policy languages instead, but at they are not equipped with an adequate semantic model.

This work in progress tries to scale the semantic approach to a very expressive class of policies. Our compositional language provides a structured way to represent the conditions that trigger the erasure process, and relates them with a precise quantification of its outcome.

All aspects of the erasure mechanism are made explicit, including assumptions about the context the system is acting into, in such a way the comparison among policies is now simple and intuitive.