A User Model for Information Erasure

Filippo Del Tedesco
Department of Computer Science and Engineering
Chalmers University of Technology

David Sands
Department of Computer Science and Engineering
Chalmers University of Technology

Abstract

There are many settings in which users are supposed to provide confidential information to an IT system for a specific purpose, on the understanding that it will be erased once that purpose has been fulfilled.

Since there are many direct and indirect ways to retain such kind of information, a formal approach to build an erasing environment is necessary.

From a high level point of view, there are two class of entities involved in such problem. The first is composed by agents which are supposed to process confidential information, namely the IT systems. For those agents we require that after they claim erasure is performed, they have to behave in a way which does not depend on secrets received.

But there are also issues related to the providers of confidential information (users), because they share with the system the responsibility of using such data in an appropriate way.

In [1] authors achieve an important result towards the understanding of erasure, giving a semantic notion of the problem for the system side, together with a type system which enforces such property in a simple imperative language with communication primitives. This feature of the language is one of the key aspects in their contribution, because only assuming a dynamic environment allow us to reason about erasing confidential information.

But despite the emphasis on this interactive view of erasure, they do not develop an explicit model of the users of the system and, as a consequence, certain requirements about the users are described but not formalized.

This is exactly the goal of this work, in which we perform the first step to enrich the user side of the erasure model.

First of all we develop a formal description of an user of the system, which is abstract enough to encompass e broad class of real users, but still suitable to handle confidential data in a noninterference style.

Then we try to define a proper behavior for users in such erasure related context: this is achieved by defining a set of semantics constraints which are specific for the class of what we called "erasure friendly" users.

With a precise notion for both user and system we are then able to formalize a global notion of erasure (which turns out to be a coherent extension of the input erasure defined in [1]) and finally we can show that each erasure friendly user can be composed together with an erasing system to obtain an environment which is jointly erasing.

As a result of the formalisation of the user we also discovered additional obligations required on erasure friendly users which where not described in [1].

Although the scenario modeled in our work is a simplification of the original version, hence many others aspects would be necessary to formalize the problem for a wider class of contexts, our results provide some useful remarks about relation between users and system trying to behave in an erasure-like way, and also can lead to strategies to lift the behavior of an arbitrary user to a proper erasure-friendly one.

References

[1] S. Hunt & D. Sands (2008): *Just Forget it – The Semantics and Enforcement of Information Erasure.* In: *Programming Languages and Systems. 17th European Symposium on Programming, ESOP 2008*, number 4960 in LNCS. Springer Verlag, pp. 239–253.