Dimensions of Declassification in Theory and Practice

Andrei Sabelfeld

Dept. of Computer Science and Engineering, Chalmers University of Technology
412 96 Gothenburg, Sweden

Abstract. Computing systems often deliberately release (or declassify) sensitive information. A principal security concern for systems permitting information release is whether this release is safe: is it possible that the attacker compromises the information release mechanism and extracts more secret information than intended? While the security community has recognized the importance of the problem, the state-of-the-art in information release is, unfortunately, a number of approaches with somewhat unconnected semantic goals. We provide a road map of the main directions of current research, by classifying the basic goals according to *what* information is released, *who* releases information, *where* in the system information is released, and *when* information can be released. We apply this classification in order to evaluate the security of a case study realized in a security-typed language: an implementation of a non-trivial cryptographic protocol that allows playing online poker without a trusted third party. In addition, we identify some prudent principles of declassification. These principles shed light on existing definitions and may also serve as useful "sanity checks" for emerging models.

The talk is based on joint work, in part, with David Sands, and, in part, with Aslan Askarov.

I. Cervesato (Ed.): ASIAN 2007, LNCS 4846, p. 1, 2007.