Title: Autonomy in Information Flow Control

Chandrika Bhardwaj
Department of Computer Science and Engineering
IIT Delhi

Abstract

Traditional mechanisms such as cryptography and access control impose limits on the information that is released by a system, but they provide no guarantees about information propagation. Information Flow Control (IFC), addresses the latter by tracking and controlling the flow of sensitive data in a system to ensure that it is not revealed or disclosed in violation of predetermined policies. We study the limitations of the state-of-the-art IFC mechanisms from the perspective of autonomy in specifying and enforcing IFC policies.

First, we propose a Lagois connection framework that permits different organisations to exchange information while maintaining both security of information flow as well as their autonomy in formulating and maintaining security policies. We show that our framework is semantically sound and that it is durable and versatile in establishing, maintaining, and repairing the desired security properties when the individual organisations change their policies or internal security class organisations. We additionally extend the proposed secure connections framework to another dimension, namely autonomy among individuals by applying it to the Decentralised Labels Model [Myers et al, SOSP'97]. Both of these contributions solve a largely open problem so far.

Next, we propose an Attribute-Based Control of Information Flow (ABCIF) framework to provide autonomy across different relationships between principals. We perform an elaborate case study and show that DIFT's [Lourenco et al, POPL'15] treatment of the parameterized lattice order can lead to counterintuitive results. We then specify a methodology for the construction of a correct security lattice model and prove that flows permitted in it are sound with respect to the credential-based semantics proposed in the thesis. This semantic interpretation allows for a very careful case analysis of the lattice order, which the "value" view of parameterization (used in DIFT) does not even afford and fixes the issues with DIFT. The ABCIF model does not, however, support features of the delegation of authority and de-classification. Thus, we propose a Decentralized Attribute-Based Control of Information Flow (DABCIF) model, in which the authorisation is not unconditional but is contextual and delimited by relationships within an organisation.

We also design and implement a middleware framework, SIFT, for systematically and automatically annotating data with security classes so that

users are relieved of having to create tags for each class of data and metadata that is collected in the system, thus making it user-friendly and scalable.