Epistemic Logic For Information Flow Security

Musard Balliu*

Abstract

Noninterference and its derivatives, for instance for declassification, are strong security properties enforcing confidentiality and integrity. The properties state that highly sensitive inputs should not influence the publicly observable behavior of a process, in order to prevent an attacker to learn sensitive information by observing public outputs. The majority of verification mechanisms for noninterference try to ensure that there is a strict separation between a computation (or slice) on sensitive inputs and another one generating the public outputs. For many programs such a strict separation is, however, not possible. This paper follows a different approach. The goal here is to reason about the dynamically varying knowledge as conveyed by a trace of public outputs. The paper presents a computational model and an epistemic temporal logic used to reason about knowledge acquired by observing program outputs. This approach is shown to elegantly capture both the standard notions of noninterference and declassification as well as information flow properties where sensitive and public data intermingle in delicate ways.

*Joint work with Mads Dam and Gurvan Le Guernic