A Weakest Precondition Approach to Robustness*

Musard Balliu
School of Computer Science and Communication
Royal Institute of Technology
Stockholm, Sweden

May 7, 2010

Abstract

With the increasing complexity of information management computer systems, security becomes a real concern. E-government, web-based financial transactions or military and health care information systems are only a few examples where large amount of information can reside on different hosts distributed worldwide. It is clear that any disclosure or corruption of confidential information in these contexts can result fatal. Information flow controls constitute an appealing and promising technology to protect both data confidentiality and data integrity. The certification of security degree of a program that runs in untrusted environments still remains an open problem in the area language-based security. Robustness asserts that an active attacker, who can modify program code in some fixed points (*holes*), is unable to disclose more private information than a passive attacker, who merely observes unclassified data. In this paper, we extend a method recently proposed for checking declassified non-interference in presence of passive attackers only, in order to check robustness by means of weakest precondition semantics. In particular, this semantics simulates the kind of analysis that can be performed by an attacker, i.e., from public output towards private input. The choice of semantics allows us distinguish between different attacks models and characterize the security of applications in different scenarios.

Our results are sound to address confidentiality and integrity of software running in untrusted environments where different actors can distrust one another. For instance, a web server can be attacked by a third party in order to steal a session cookie or hijack clients to a fake web page.

*Joint work with Isabella Mastroeni, University of Verona, Italy.