

Filippo Del Tedesco, Chalmers University of Technology, Göteborg.

Title: Implementing Erasure Policies Using Taint Analysis

Abstract:

A growing number of security-critical services are already available on-line. Every day users provide data about their credit cards, email addresses, phone numbers, etc. Among the many desirable properties, systems that handle those data should not be allowed to retain some information after it has been used for some purpose. For example, once users pay bills using credit cards, commercial sites should not record credit cards information for a future use. Security policies regarding what, and when, information should be deleted is known as information-erasure policies. In this talk we present a library to handle information-erasure policies for Python programs. The library is based on the well-known concept of taint analysis that is frequently used to address confidentiality issues in programs. Essentially, the library acts on each piece of data assigning additional information specified by a information-erasure policy, in order to indicate when it should be deleted or forgotten. In addition, the library keeps track of how erasure-related information is propagated inside the program. In this manner, the library can guarantee that information that should be deleted at some point in time, as well as any other data derived from it, is actually erased. The library is lightweight, easy to use, and allows programmers to indicate information-erasure policies with minor modifications in the code. To the best of our knowledge, this is the first implementation of a library that connects taint analysis and information-erasure policies. This talk is based on a joint-work-in-progress with David Sands and Alejandro Russo.