Security through Static Analysis

Chris Hankin

Our thesis is that static analysis provides an important, but largely unexploited, collection of tools for the automated verification of programs that are expected to obey some security protocol. This thesis is being developed in the context of the EU-funded FET project SecSafe. This talk will start with a brief overview of the project. The main content of the presentation will focus on the flow-logic style of specification of static analyses. We will illustrate this, which is one of the main approaches being pursued in SecSafe, with reference to Information Flow Analysis for simple imperative languages. The talk will conclude with perspectives for future work with, if time permits, a brief review of our current work on quantitative approaches to security.