Andrew Myers

30 mars 2011

Constructive Security Using Information Flow Control

Abstract:

I describe the use of information flow control to build secure distributed computing systems. This is a constructive approach to security in the sense that the process of constructing the software gives assurance that it is secure. Experience shows a constructive approach is needed: it is too difficult to analyze the security of systems after they are built. In the constructive approach, programmers annotate their code with security policies describing the confidentiality and integrity of the data they manipulate. The compiler and run-time system analyze and transform the code to ensure that it does not contain insecure information flows. This approach can even be applied to the construction of secure federated systems, distributed systems in which the participants do not fully trust one another. An added benefit of this approach is that the level of abstraction for building distributed systems is raised. For example, in the Swift web application framework, annotated code is securely and automatically partitioned between the Web server and the client browser. The Fabric system introduces a more general, high-level abstraction for building complex federated information systems securely, reliably, and efficiently.