Software Security by Information Flow Control

David Sands
Chalmers University of Technology, Gothenburg, Sweden

A long term goal is to construct innovative design methods for the construction of secure systems that put security requirements at the heart of the construction process, namely *security by design*. To do this we must

(i) understand how we can unambiguously formulate the policy aims for secure systems, and

(ii) develop technology to integrate these goals into design mechanisms and technologies that enables an efficient construction or verification of systems with respect to those policies.

In this course we will explore security and privacy policies for data manipulated by software. Certain security policies, for example access control, are relatively easy to express in many modern programming languages. This is because limiting access to resources is something that good programming language abstraction mechanisms are designed to handle. However, access control mechanisms are often a poor tool to express the end-to-end security requirements that we actually want from applications.

In the course we will

(i) better understand the semantics of information flow,

(ii) explore dynamic and state-dependent policies,

(iii) see how these ideas can be incorporated into a programming language with support for static verification of a rich variety of information flow policies.

We will also look at differential privacy - a theoretically popular approach to formulating privacy which gives strong guarantees. We will explore how the dynamic tracking of information flow can enforce differential privacy for programs operating over sensitive databases.

Background Material

[1] A. Sabelfeld, A. C. Myers. *Language-Based Information-Flow Security*. IEEE Journal on Selected Areas in Communications, Vol. 21; 2003.
`http://www.cse.chalmers.se/ andrei/sabelfeld-myers-isss03.pdf`

[2] C. Dwork. *A Firm Foundation for Private Data Analysis*. Communications of the ACM; Association for Computing Machinery, Inc.; 2011.
`http://research.microsoft.com/pubs/116123/dwork_cacm.pdf`.

[3] *David Sands's Publications*.
`http://www.cse.chalmers.se/ dave/davewww.html`