Software Security by Information Flow Control

David Sands
Chalmers University of Technology, Göteborg, 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*. But to do this we must

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

(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 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. For example consider a travel planner "app" which permits you to plan a bus journey, and even add your planned bus route to your calendar. In order to function, the app must have access to the network to fetch the latest bus times, and must have access to your calendar in order to add or remove schedules. But an app with these permissions can, for example, send your whole calendar to anywhere on the net. What we want is to grant access to these resources, but limit the *information flows* that the app permits. In this case we want to at least limit the information flows from the calendar to network while retaining the app's ability to read and write to both.

In the course we will

(i) better understand the semantics of information flow,

(ii) explore dynamic and state-dependent policies, and

(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.

References

[1] G.McGraw, G.Morrisett. *Attacking Malicious Code: A Report to the Infosec Research Council.* IEEE Software, Vol. 17(5), pp. 33–41, IEEE Computer Society Press, 2000.
`http://www.cs.cornell.edu/Info/People/jgm/lang-based-security/maliciouscode.pdf`

[2] A.Sabelfeld, A.C.Myers. *Language-Based Information-Flow Security.* IEEE Journal on Selected Areas in Communications, Vol. 21, pp. 5–19, 2003.
`http://www.cse.chalmers.se/ andrei/sabelfeld-myers-isss03.pdf`

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