Colloquium d'Informatique de l'UPMC Sorbonne Universités

Desperately seeking software perfection

Xavier Leroy, Inria

Amphi 25

4, place Jussieu
75005 Paris
Metro Jussieu

**20 Octobre 2015
à 18h00**

In the general public, "software" has become synonymous with "bugs" and "security holes". Yet, there exists life-critical software systems that achieve extraordinary levels of reliability, as I'll illustrate with fly-by-wire systems in airplanes. A recent development in this area is the introduction of tool-assisted formal verification (static analysis and program proof) to complement, and sometimes replace, traditional test-based verification. However, the assurance provided by formal verification is limited by the confidence we can have in the verification tools and in the compilers that produce actual executables from verified sources. Using the CompCert verified C compiler as an example, I'll show the effectiveness of formally verifying, with the help of proof assistants, the tools that participate in the construction and verification of critical software.

Xavier Leroy is a senior research scientist at Inria Paris where he leads the Gallium research team. His research focuses on programming languages and tools, and on the formal verification of software using program proof and static analysis. He is the architect and one of the main developers of the OCaml functional programming language and of the CompCert formally-verified C compiler.

contact : colloquium@lip6.fr
http://www.lip6.fr/colloquium/
Vidéo disponible sur le site

cnrs

LIP6

UPMC
SORBONNE UNIVERSITÉS