SÉMINAIRE #1 MERCREDI 16/09/2020 PAR DAVID PICHARDIE : FORMAL VERIFICATION OF A CONSTANT-TIME PRESERVING C COMPILER

le 16 septembre 2020 17h30-18h30

ENS Rennes En distanciel sur ce serveur BigBlueButton

Intervention de David Pichardie, professeur des universités à l'ENS Rennes, chercheur dans l'équipe CELTIQUE de l'IRISA et Inria Rennes, dans le cadre des séminaires du département Informatique et télécommunications.

Timing side-channels are arguably one of the main sources of vulnerabilities in cryptographic implementations. One effective mitigation against timing side-channels is to write programs that do not perform secret-dependent branches and memory accesses. This mitigation, known as "cryptographic constant-time", is adopted by several popular cryptographic libraries.

This work focuses on compilation of cryptographic constant-time programs, and more specifically on the following question: is the code generated by a realistic compiler for a constant-time source program itself provably constant-time? Surprisingly, we answer the question positively for a mildly modified version of the CompCert compiler, a formally verified and moderately optimizing compiler for C. Concretely, we modify the CompCert compiler to eliminate sources of potential leakage. Then, we instrument the operational semantics of CompCert intermediate languages so as to be able to capture cryptographic constant-time. Finally, we prove that the modified CompCert compiler preserves constant-time. Our mechanization maximizes reuse of the CompCert correctness proof, through the use of new proof techniques for proving preservation of constant-time. These techniques achieve complementary trade-offs between generality and tractability of proof effort, and are of independent interest.

/**/ td {border: 1px solid #ccc;}br {mso-data-placement:same-cell;}</style> <br class="separateur" /> <!-- #description /**/

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

À TÉLÉCHARGER

Séminaire DIT #1 16/09/20 par David Pichardie (PDF, 2467 Ko)

À LIRE AUSSI

Séminaire #2 mercredi 30/09/2020 par Stéphanie Challita

Séminaire #3 mercredi 04/11/2020 par Ocan Sankur : An Abstraction Technique for Parameterized Model Checking of Leader Election Protocols: Application to FTSP

Séminaire #4 mercredi 02/12/2020 par Claire Cury

DOCUMENTATION

Vous souhaitez recevoir plus d'information sur l'ENS Rennes, vous pouvez pour cela remplir leformulaire de demande de documentation.