Pas de Pannes, Pas d'Exploits: Vérification Automatique de Noyaux Embarqués

Olivier Nicole[1], Matthieu Lemerre[1], Sébastien Bardin*[1], and Xavier Rival[2]

[1]CEA LIST – Université Paris Saclay, Université Paris-Saclay – France
[2]Département d'informatique de l'ENS – Ecole Normale Supérieure de Paris - ENS Paris, CNRS : UMR8548, PSL University, Inria Paris – France

Résumé

Rejeu de la publication suivante acceptée à RTAS 2021 :
No Crash, No Exploit: Automated Verification of Embedded Kernels
The kernel is the most safety- and security-critical component of many computer systems, as the most severe bugs lead to complete system crash or exploit. It is thus desirable to guarantee that a kernel is free from these bugs using formal methods, but the high cost and expertise required to do so are deterrent to wide applicability. We propose a method that can verify both absence of runtime errors (i.e. crashes) and absence of privilege escalation (i.e. exploits) in embedded kernels from their binary executables. The method can verify the kernel runtime independently from the application, at the expense of only a few lines of simple annotations. When given a specific application, the method can verify simple kernels without any human intervention. We demonstrate our method on two different use cases: we use our tool to help the development of a new embedded real-time kernel, and we verify an existing industrial real-time kernel executable with no modification. Results show that the method is fast, simple to use, and can prevent real errors and security vulnerabilities.

*Intervenant