Formal Methods for Systems Security

Wan Fokkink, Cristiano Giuffrida, Herbert Bos

Formal methods are being successfully applied in the realm of security, notably in the analysis of network protocols. However, security vulnerability of computer systems nowadays occur more and more at the hardware level. A poignant example is the recent string of cache side-channel attacks, which exploit minimal information leakage via caches. Or the sensational exploits of speculative execution, where microprocessors do work in advance, to prevent delay in case the work is actually needed later; if it turns out the work is not needed, changes are reverted and results are ignored. Notable recent attacks that target microprocessors are Meltdown, Spectre and TLBleed. And at the software level, software patches, which often aim to repair security leaks, tend to introduce new security vulnerabilities that go undetected by software developers.

Formal methods are of the essence to help in harnessing computer systems against such low-level attacks. For this, first of all formal models need to be developed that are at a sufficiently abstract level to obtain general correctness results, but at a sufficiently detailed level to analyze and guarantee security properties at the hardware level. Notably, the CacheAudit tool for static analysis of cache side channels developed by Boris Köpf and his co-workers is an interesting first step in this direction. The groundbreaking work of the team of Gernot Heiser at NICTA, on the microkernel seL4 that was verified using Isabelle/HOL, can also be considered a road map for achieving firm security guarantees at the system level through formal verification. The work has reached sufficiently mature levels to allow for adoption in real-world systems. Such and similar work at MIT and other places on reliable and secure file systems, compilers and other components of low-level systems indicate both a growing trend in research in the space between systems security and formal methods and an increasing need for such research.

The security and formal methods groups in the department of computer science at the Vrije Universiteit Amsterdam are joining forces and work on formal methods for systems security. A first result of this collaboration is the master thesis of Kevin Maiutto from August 2018, in which the TLBleed attack has been analyzed using CacheAudit. The long-term plan for this effort is to generalize the current framework to several classes of side-channel attacks and model arbitrary defenses as constraints on the underlying formal model. More broadly, focus points for the coming years are formally reasoning over the properties of side channel attacks in the memory subsystem and guaranteeing the correctness of software patches.