AppControl/ES3C: Enforceable Specifications for Secure Systems-on-Chip

Wim Vanderbauwhede (Glasgow), Nobuko Yoshida (Imperial), Klaus McDonald-Maier (Essex)

22 November 2019

The Problem: Controlling Behaviour

- It is possible to limit the access privileges of a third-party program running on a computer system.
- Architectural capabilities enable unprecedented fine-grained memory protection and isolation.
- But how to ensure that the program follows the intended specification?

Our Aim

- Provide Digital Security By Design for mission-critical Systems-on-Chip through Design-by-Specification.
- Our vision: a SoC has a formal, executable specification;
  - Every component of the SoC, software or hardware, has to adhere to this specification.
  - Programs with incompatible specifications cannot run
  - Unspecified runtime behaviour will raise an exception.

Key Ideas in a Nutshell

- Make use of behavioural type system: specification of the SoC and each of its components are expressed as a type
- This type effectively and formally describes the allowed interfaces and interactions of each component.
  - an integral component of the program executable
  - validated against an overall system specification by the operating system.
- This proposal focuses on software components,
- We will build on the capability hardware for enforcement of the type-based specifications.

Specifications: Interfaces and Behaviours