Border Patrol

Improving Hardware Security through Type-Aware Systems Design

Dr. Wim Vanderbauwhede, University of Glasgow
Prof. Sven-Bodo Scholz, Heriot-Watt University
Prof. Nobuko Yoshida, Imperial College London

https://border-patrol.github.io/

There are increasing concerns about the safety and security of critical infrastructure such as nuclear power plants, the electricity grid and other utilities in the face of possible cyber attacks. As ageing controllers are replaced by smart devices based on Field-Programmable Gate Arrays and embedded microprocessors, the safety of such devices raises many concerns. In particular, there is the very real risk of malicious functionality hidden in the silicon or in software binaries, dormant and waiting to be activated. Current hardware and software systems are of such complexity that it is impossible to test all parts of the systems to discover such code.

We aim to address this problem by closely connecting the system design specification with the actual implementation through the use of a formal design methodology based on type systems with static *and dynamic* type checking. The type system will be used as a formal language to encode the design specification so that the actual implementation will automatically be checked against the specification.

Static type checking of data types and multiparty session types can ensure the correctness of the interaction between the components. However, as static checking assume full access to the design source code it cannot be used to protect against potential threads issuing from third-party functional blocks (know as 'Intellectual Property Cores' or IP cores) that are commonly used in hardware design: the provider of the IP core can *claim* adherence to the types and protocols, so that the IP core will meet the compile-time requirements, but the run-time behaviour cannot be controlled using static techniques. The same applies to third-party compiled software libraries. Therefore we propose to use run-time checking of data types as well as session types at the boundaries of untrusted modules (*Border Patrol*) so that any intentional or unintentional breach of the specification will be safely intercepted.

For more details contact:

Dr. Wim Vanderbauwhede (Principle Investigator) wim.vanderbauwhede@glasgow.ac.uk University of Glasgow