A hardware coprocessor for Zynq-based Dynamic Information Flow Tracking

Muhammad Abdul Wahab[α], Pascal Cotret[α], Mounir Nasr Allah[β], Guillaume Hiet[β]
Vianney Lapôtre[γ], Guy Gogniat[γ]
[α] IETR / SCEE research group, firstname.lastname@centralesupelec.fr
[β] INRIA / CIDRE research group, firstname.lastname@centralesupelec.fr
[γ] Lab-STICC / University of South Brittany, firstname.lastname@univ-ubs.fr

This talk introduces an efficient and portable approach for DIFT (*Dynamic Information Flow Tracking*) implementations on reconfigurable chips. DIFT aims to track the application control flow by adding metadata (also known as tags) to information containers (e.g. registers, memory addresses, ...), propagating and checking it at runtime. These approaches have been successfully used against a wide range of attacks including buffer overflow, SQL injections and so on.
Existing DIFT solutions are either hardly portable or bring unsatisfactory time overheads. For example, DIFT in software brings an overhead of at least 300% and can rise up to 3700%. Our chosen approach conists of using a dedicated coprocessor to decouple main computation (application) from tags computation. To efficiently retrieve information on executed instructions by the main CPU, ARM Coresight components are used to export CPU trace towards FPGA part of Zynq SoC. In addition to trace, static analysis needs to be done to get dependencies between information containers. This talk will present our chosen approach, ongoing work on first prototype and first results. Existing DIFT approaches and ARM Coresight components will also be discussed.