PhD proposal - Combining static analysis with hardware-assisted Dynamic Information Flow Control

Title: Combining static analysis with hardware-assisted Dynamic Information Flow Control.
Funding: HardBlare project funded by Labex CominLabs.
Period: From October 2015 to September 2018 (36 months).
Location: Rennes (Brittany, France) in CentraleSupélec Inria CIDRE research team. Maybe some travels to Lab-STICC team in Lorient (Brittany, France).
Advisors: Dr. Guillaume Hiet (Rennes), Dr. Pascal Cotret and Pr. Guy Gogniat (Lorient).
Keywords: Hardware/software co-design, security, information flow control, static and dynamic analysis.
Collaboration: This PhD is part of the HardBlare project, a multidisciplinary project between CentraleSupélec IETR SCEE research team, CentraleSupélec Inria CIDRE research team and UBS Lab-STICC laboratory. Lab sites:
SCEE team: `http://www.rennes.supelec.fr/ren/rd/scee/`
CIDRE team: `http://www.rennes.supelec.fr/ren/rd/cidre/`
Lab-STICC team: `http://www.labsticc.fr/`

Context and motivations

The general context of the HardBlare project is to address Dynamic Information Flow Control that generally consists in attaching marks to denote the type of information that is saved or generated within the system. These marks are then propagated when the system evolves and information flow control is performed in order to guarantee a safe execution and storage within the system. Existing solutions imply a large overhead induced by the monitoring process. Some attempts rely on a hardware-software approach where DIFC operations are delegated to a coprocessor. Nevertheless, such approaches are based on modified processors. Beyond the fact hardware-assisted DIFC is hardly adopted, existing works do not take care of coprocessor security and implementation and multicore/multiprocessor embedded systems.
We plan to implement DIFC mechanisms on boards including a non-modified ARM processor and a FPGA such as those based on the Xilinx Zynq family.
More details about the whole HardBlare project can be found at:
`https://pascalcotret.files.wordpress.com/2015/02/hardblare_proposal.pdf`

PhD objectives

- **State of the art analysis.** The first objective is to analyze the previous relevant works and implementations about static and dynamic IFC solutions (including Blare tools developed at SUPELEC CIDRE). A second objective is to study some works about hardware-assisted DIFC and hardware/software co-design.

- **Combination of static and dynamic analysis.** We will study how hybrid analysis can be used in the context of the HardBlare project (especially regarding dependencies with the hardware layer of the project).
- **First demonstrator.** At this stage, the PhD student will collaborate with another PhD focused on hardware issues in the HardBlare project. The main goal is to build a prototype where the DIFC hardware/software system will rely on a non-modified general purpose processor. Once this demonstrator will be implemented, its efficiency will be compared with existing solutions.
- **Persistence management for DIFT.** The main goal of this task will be to study how we can provide tainting for mass storage, i.e. files, in order to provide confidentiality/integrity to the whole system. This persistent tag management is necessary to maintain the security level when the system is rebooted.

Requirements

- Computer security, dynamic and static analysis (some knowledge about Information Flow Control is a plus).
- Knowledge on operating systems development (C/C++, GNU/Linux environment).
- Basic knowledge on embedded systems and computer architectures.

Application

The applicant must hold a Master degree in computer science, digital electronics or a related field. Please provide the following documents as a single ZIP archive to all three contacts found below:

- Curriculum of the applicant.
- Detailed motivation letter with skills corresponding to the PhD thesis.
- If possible : grades and rankings of previous degrees, recommandation letter(s) from previous advisor(s) (with their complete name and coordinates as they may be contacted).

Contacts

Guillaume Hiet
CentraleSupélec, Rennes campus
guillaume.hiet@centralesupelec.fr

Pascal Cotret
CentraleSupélec, Rennes campus
pascal.cotret@centralesupelec.fr

Guy Gogniat
Lab-STICC, University of South Brittany, Lorient campus
guy.gogniat@univ-ubs.fr

References

[1] S. Chiricescu, A. DeHon, D. Demange, S. Iyer, A. Kliger, G. Morrisett, B.C. Pierce, H. Reubenstein, J.M. Smith, G.T. Sullivan, A. Thomas, J. Tov, C.M. White, and D. Wittenberg. Safe: A clean-slate architecture for secure systems. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 570–576, Nov 2013.

[2] Michael Dalton, Hari Kannan, and Christos Kozyrakis. Raksha: A flexible information flow architecture for software security. In *Proceedings of the 34th Annual International Symposium on Computer Architecture*, ISCA '07, pages 482–493, New York, NY, USA, 2007. ACM.

[3] H. Kannan, M. Dalton, and C. Kozyrakis. Decoupling dynamic information flow tracking with a dedicated coprocessor. In *Dependable Systems Networks, 2009. DSN '09. IEEE/IFIP International Conference on*, pages 105–114, 2009.

[4] Hari Kannan. Ordering decoupled metadata accesses in multiprocessors. In *Proceedings of the 42Nd Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO 42, pages 381–390, New York, NY, USA, 2009. ACM.

[5] G. Edward Suh, Jae W. Lee, David Zhang, and Srinivas Devadas. Secure program execution via dynamic information flow tracking. In *Proceedings of the 11th International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS XI, pages 85–96, New York, NY, USA, 2004. ACM.

[6] Guru Venkataramani, Ioannis Doudalis, Yan Solihin, and Milos Prvulovic. Flexitaint: A programmable accelerator for dynamic taint propagation. In *In 14th International Symposium on HighPerformance Computer Architecture (HPCA-14*, 2008.