PhD Position: Runtime Threat Prediction

The MOCS team at Lab-STICC ENSTA-Bretagne is searching for a young, motivated and skilled PhD researcher with a strong background in computer science and engineering.

Position: PhD student
Duration: 36 months *starting date:* as soon as possible
Requirements: Master + European citizen
Where: MOCS team at Lab-STICC ENSTA-Bretagne, Brest
Scientific advisors: Loïc LAGADEC, Ciprian TEODOROV, Youri HELEN

About Lab-STICC ENSTA-Bretagne

ENSTA Bretagne was founded in 1971 and is a multidisciplinary engineering institute under the auspices of the French Defence Ministry (DGA). ENSTA Bretagne has established itself in the field of IT oriented research, thought its laboratory Lab-STICC (UMR 6285), standing for ”Information and Communication Science and Technology Laboratory. Lab-STICC is a French National Centre for Scientific Research (CNRS) mixed unit shared with two universities and two other engineering institutes.
Lab-STICC’s focus can be summed up in the following motto: COMMUNICATE and DECIDE « from sensor to knowledge » standing for bringing solutions for physical layers at radio-frequency level, designing data transmission and management systems based on advances in both algorithmic and micro-electronic fields, and analyzing information to deliver knowledge to final users.
Lab-STICC ENSTA Bretagne has been developing several tools that perform system level design and verification (OBP, http://www.obpcdl.org/), high-level synthesis (Morphose), and low-level reconfigurable architecture modelling & design kit (Madeo), that are currently being retargeted to security concerns.

Context

Embedded systems are, today, at the hearth of most complex systems and the tendency is towards an increased reliance on the use of dynamically “programmable” software and architectures even in security-critical systems. In this context, the French government emphasizes the need to acquire a nation-wide capability in the field of cyber-security enabling the protection against cyber-attacks of vital infrastructures and systems.
Traditionally, in the case of critical embedded systems, the design and production process follows a very strict system engineering discipline to guarantee the quality of the solution with respect to the formalized requirements. However, as these systems interact with their operational environment it is hard to exhaustively capture the dynamic behavior of the environment and to statically prove the safety requirements of the system in its real operational environment. Moreover, if the system is “supposed” to operate in an adverse environment the static verification becomes virtually impossible due to the existence of un-anticipated environment behaviors (e.g. unknown attack scenarios).
Typical attack scenarios consist in voluntary changing the behavior of a system by introducing environmental perturbation outside of the “allowed” and guaranteed operational ranges (electromagnetic attacks, out-of-range temperature and pressure conditions, etc). The emerging behavior of the systems in such conditions is hard to predict. However, in the case of reactive control systems, there is a “temporal window” between the start of the divergent environment

action and the reaction of the system. This “temporal window” offers the possibility to dynamically reconfigure the system in a protected mode before the concretization of the attack. This dynamic reconfiguration of the system is based on the runtime anticipation of threats, and its principal requirement is that the “protective reaction” should occur during the “temporal window” and not afterwards.

Research Topic

In the context of software system, there is a large research body studying attack detection and prediction at the application and system-level [1]. In the integrated circuits (IC) domain, however, most of the research efforts are geared either towards the study of low-level security mechanisms (cryptography, physically un-clonable functions, etc.) or towards technological security solutions (side-channel attacks, etc.). The globalization of system-on-chip (SoC), however, widens the security requirements to include the need for efficient and scalable attack detection and prediction methods at the hardware-level [2]. The project SAFES [3], for instance, integrates system-level attack detection in a SoC architecture with high-security guarantees. Nevertheless, most of the solutions today rely on the monitoring of secondary witness variables, like the energy consumption, that implies that a potential attack is detected only after it influences the witness variables. The principal drawback of these approaches is that the detection happens after the concretization of the attack in the system.
This thesis strives to address this problem by the introduction of a configurable prediction system capable of anticipating a threat before it starts to impact behavior of the protected system. The prediction module, inspired by formal exhaustive verification techniques [4, 5], would be a hardware module integrated in a SoC. It would be able to exhaustively check the reaction of the embedded SoC controller to the operational environment up to a predefined security bound. This prediction phase would be parallel to the real-execution phase and would enable the detection of a potential threat before its concretization on the real execution.

Some related research problems addressed by the MOCS team at ENSTA Bretagne are: high-level circuit synthesis [6, 7, 8], reconfigurable system-on-chip design [9], security verification through online hardware monitoring [10], and environment-driven formal verification [11].
The MOCS team at ENSTA-Bretagne has exclusive access to a high-performance FPGA platform and one high-performance in-memory super-computer, which would offer the needed infrastructure for performing quantitative and qualitative evaluations on industrial case-studies to validate the scientific hypotheses and the results obtained.

References:

[1] F. Salfner, M. Lenk, and M. Malek. 2010. A survey of online failure prediction methods. ACM Comput. Surv. 42, 3, Article 10 (March 2010), 42 pages.
[2] B. Badrignans, J-L. Danger, V. Fischer, G. Gogniat, and L. Torres. 2011. Security Trends for FPGAS: From Secured to Secure Reconfigurable Systems. Springer.
[3] G. Gogniat, T. Wolf, W. Burleson, J. P. Diguet, L. Bossuet and R. Vaslin, "Reconfigurable Hardware for High-Security/ High-Performance Embedded Systems: The SAFES Perspective," in IEEE Transactions on VLSI Systems, vol. 16, no. 2, pp. 144-155, 2008.
[4] M.E. Fuess, M. Leeser, T. Leonard, "An FPGA Implementation of Explicit-State Model Checking," in Field-Programmable Custom Computing Machines, 2008. FCCM '08. 16th International Symposium on , vol., no., pp.119-126, 14-15 April 2008.
[5] A. Biere, A. Cimatti, E.M. Clarke, O. Strichman, Y. Zhu, “Bounded model checking”. Advances in computers, 58, 117-148, 2003.
[6] L. Lagadec, B. Pottier, Object-oriented meta tools for reconfigurable architectures. Proc. SPIE 4212, Reconfigurable Technology: FPGAs for Computing and Applications II, 69, 2000.

[7] P. Coussy, C. Chavet, P. Bomel, D. Heller, E. Senn, E. Martin, “Gaut: A high-level synthesis tool for DSP applications”. In P. Coussy and A. Morawiec, editors, High-Level Synthesis, pages 147–169. Springer Netherlands, 2008.
[8] L. Lagadec, D. Picard, and B. Pottier. Dynamic System Reconfiguration in Heterogeneous Platforms: The MORPHEUS Approach, chapter Spatial Design, pages 165–182. Springer Netherlands, 2009.
[9] L. Lagadec, C. Teodorov, J.-C. L. Lann, D. Picard, and E. Fabiani. Model-driven toolset for embedded re- configurable cores: Flexible prototyping and software-like debugging. Science of Computer Programming, 96, Part 1:156 – 174, 2014.
[10] M. Ben Hammouda, P. Coussy, L. Lagadec, “Design Approach to Automatically Synthesize ANSI-C Assertions during High-Level Synthesis of Hardware Accelerators”, ICSAS - International symposium on circuits and systems, 2014
[11] C. Teodorov, P. Dhaussy, L. Le Roux, “Environment-driven reachability for timed systems”, International Journal on Software Tools for Technology Transfer, pp.1-17, 2015.