Proposition de recherche doctorale

High-level Assurance of Connected Devices by Composition Verification

Mots clés :

- **Directeur de thèse** : Emmanuelle Encrenaz
- **Co-encadrant(s)** :
- **Unité de recherche** : Laboratoire d'informatique de Paris 6
- **Ecole doctorale** : École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

Résumé du projet de recherche (Langue 1)

{{Context}}. The trustworthiness of the Internet of Things is being ensured by the critical connected devices composing of embedded software running on a SoC such as secure element, TEE , TPM , smart-meters, wireless sensors, etc. These devices usually work in a hostile environment and are submitted to numerous attacks. In this stage, the security functions provided by the device must be correctly implemented. On the other hand, these security functions must also be sufficiently robust with respect to the attacks i.e. the integrated counter-measures should be effective (in the corresponding attack models). Currently, the industrial approach for evaluating the correctness of the security functions is mainly based on the functional test suites defined on the external interfaces of the device. The functional test suites are usually built for compliance purpose and only provide a minimal level of assurance. Formal analysis enables higher assurance provided that it may handle an effective scope (such as the full device implementation). For robustness, the evaluation consists in applying a catalogue of attacks in a laboratory: a product is considered to be robust if no vulnerability has been found during a bounded time. The cost of such evaluation is high: an identified vulnerability requires fixes by the manufacturer and a re-assessment to validate them. Similarly, any modification of the product also requires a re-assessment. Meanwhile, more and more counter-measures are being invented and applied to the connected devices. Many of them are proprietary and poorly documented. Assessing the effectiveness of these counter-measures by formal analysis seems to be a promising direction. Formal analysis provides an evaluation approach based on theoretical models. These models allow the engineers to detect potential weakness before performing pen-testing. Formal analysis also provides hints to identify the potential vulnerabilities and hence, reduce the pen-testing cost (as reported in [7]). However, formal robustness analysis is a new domain which makes slow progress due to the complexity of the theoretical models. Applying formal robustness analysis to an effective scope is not expected in the near future. In the context described above, a more pragmatic method of formal analysis is necessary for industrial deployment. This method should be able to handle the complete device (i.e. the full stack of hardware and software layers). For that, we advocate to leverage the existing work (by different formal and semi-formal methods) by a modular and combination approach. The modularity is applied to the source-code and properties while the combination is applied to the analysis methods. Our objective is to get a high-level assurance by combining both formal and semi-formal evidences of the device. For example, a critical property of a critical component should be formally verified while the secondary properties of complementary components may be checked by lightweight methods such as static analysis or simulation. {{{Topic}}} This thesis is firstly aimed at enabling the formal verification of digital hardware implementation (i.e. in HDL). The verification targets the critical components such as crypto-accelerators, Master key/Boot/JTAG management, etc. For that, it is necessary to identify the class of security properties and counter-measures that may be targeted by formal analysis. For a given (hardware) component, several formal and semi-formal approaches may be combined to evaluate the robustness level of the system. One of the aims is to identify the right approach for a particular property. Then, one can derive, for a component, a verified set of security properties, which may be re-used in a larger context, adopting a compositional reasoning. The compositional verification of a secure embedded system, seen as a combination of stacked hardware and software layers is the second objective of this thesis : based on the verification of each component and the sets of properties attached to each of them (obtained from the first step), an abstraction of the whole system can be made, alleviating the verification process. The main difficulties here concern the identification of a sufficient (but not too big) set of properties to be attached to each component, which will be useful for the verification of the security properties of the whole system. Here again, several approaches can be used to combine the properties, in order to reach the high-level of assurance on a full device. An important point of the thesis is the combination of different approaches to achieve the evaluation of the device. Deductive approaches and model-checking are complementary, and the recent development of SMT solvers, which implements decidable theories, simplify the verification process of systems modeled with different classes of objects and variables. Moreover, semi-formal analysis (which can be seen as instrumented simulation) is widely used as it is the simplest way to have (partial) information about a complete SoC. All these means may be combined to get a better understanding of the security level of the analyzed system. {{{Expected Outcomes}}} The thesis is expected to generate new results (i.e. publications) by research on the formal verification of the digital hardware implementation and on the composition verification. From an industrial point of view, the expected outcome is an integrated verification environment that produces and manages the high-assurance evidences (models, proofs, traces/logs, etc) of complete connected devices (i.e. full stack of hardware and software layers). The environment leverages the verification done different formal/semi-formal tools. {{{Related work}}} Formal verification of functional properties has been applied to embedded software in both model checking (e.g. [1]) and deductive approach (e.g. [2]), and lots of works have been done on hardware components, described either in VHDL or Verilog The development of SystemVerilog and SystemC allow the designers to describe and simulate complete embedded systems, encompassing the software layers executed upon the hardware framework; however, formal approaches have difficulties to tackle such complex systems. Compositional and Abstraction approaches have been proposed for such descriptions [3, 4]), but remain under-exploited: not all properties can be analyzed by these ways, and the proof process requires a good expertise of the circuit and proof techniques ([1]). Formal methods are also used to verify security protocols and virtual platforms (KRAKATOA [5], TOOKAN [6], etc.). They have also been used to evaluate the robustness level of circuits, submitted to fault injection such as bit-flips (being generated by aggressive environments or due to physical attacks [1]). In these latest works, the complexity of the analyzed blocks is limited (less than 100 registers), and one has to develop a compositional methodology to analyze bigger systems. From an industrial point of view, while separate software and hardware components (e.g. micro-kernel , RTOS , Virtual Machines , MPU , micro-processor) have been formally verified, the verification of a full embedded system is yet to be done. In the US, the DARPA has recently launched an ambitious research program called “Secure Software Components Leveraging the seL4 Microkernel” which is aimed at verifying the software applications built upon the seL4 kernel. The objective is not to fully formalize an application but only the trusted link between it and the kernel. For mobile devices, Samsung integrated in 2014 the formally verified Green Hills RTOS in their commercial mobile security solution Knox. On the other hand, the so-called top-down approach which consists in formally modeling the system and then, generating the code is proposed for example by Prove&Run, ClearSy (Atelier-B) or Galois (Cryptol). The top-down approach integrates the formal verification very early in the product life-cycle and generates a correct-by-construction implementation. However, the generated code is weakened by its performance and is irrelevant for a manuaview (e.g. in order to add counter-measures). In additional, the top-down approach usually generates a critical component but not the complete product. Actually, top-down verification can be seen as a method to generate high-assurance evidences in our proposed environment. {{{References}}} [1] S. Baarir et al. Feasibility Analysis for MEU Robustness Quantification by Symbolic Model-Checking, In Proc. of Formal Methods in System Design, 2011. [2] M. Christo? et al. Formal veri?cation of a CRT-RSA implementation against fault attacks. J. Cryptographic Engineering, 3(3):157–167, 2013. [3] Saddek Bensalem et al. : Compositional Verification for Component-Based Systems and Application. ATVA 2008: 64-79 [4] Cécile Braunstein, Conception Incrémentale, Vérification de Composants Matériels et Méthode d'Abstraction pour Vérification de Systèmes Intégrés sur Puce, Université Pierre et Marie Curie (UPMC), 2007 [5] Claude Marché, Nicolas Rousset: Verification of JAVA CARD Applets Behavior with Respect to Transactions and Card Tears. SEFM 2006: 137-146 [6] Matteo Bortolozzo et al. : Attacking and fixing PKCS#11 security tokens. ACM Conference on Computer and Communications Security 2010: 260-269