Hardware Obfuscation Using High Level Aggregation

Gorbachov Valeriy[1]
Abdulrahman Kataeba Batiaa[1]
Ponomarenko Olha[1]
Kotkova Oksana[1]

[1]*Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, valeriy.gorbachov@nure.ua*

Abstract. *The main principle of the proposed techniques is design obfuscation method to achieve hardware security. In the work we consider the reconfigurable-based obfuscation in the post-fabrication stage of IC. We address the need to add reconfigurable-logic stage to the development cycle. This technique may be considered as a preventative measure concealing some of the design from an attacker. In other words, it hides the exact functionality and schematic of an IC until after the reconfigurable logic has been programmed.*

Keywords: *security; reference monitor; hardware design obfuscation; hardware Trojan detection; hardware Trojan prevention; countermeasures.*

I. INTRODUCTION

With increasing computing power and integration density, several issues in design, performance and manufacturing of ICs have emerged. Moreover, increasing power consumption, increased cost of testing and verification, and complexities in manufacturing devices are the some of the major issues with IC design and manufacturing. To make such design and manufacturing feasible, an IC design house is commonly aided by the following external tools: the sophisticated software tools (EDA), that facilitates design, verification and testing of modern ICs; preverified, high performance, functional hardware IPs design facilities, which help to reduce the design time, improve reliability; the fabrication facilities where the design is actually manufactured and sometimes tested.

Reduced control on the IC life-cycle emphasizes various security issues associated with ICs. Hence, security of hardware ICs has emerged as a major challenge in IC design and test.

The main goal of the research is to develop design techniques that can effectively resist or mitigate the security threats at untrusted stages of the IC life-cycle. The main principle of the proposed techniques is design obfuscation method to achieve hardware security. In the work we consider the reconfigurable-based obfuscation in the post-fabrication stage of IC. We address the need to add reconfigurable-logic stage to the development cycle. This technique may be considered as a preventative measure concealing some of the design from an attacker. In other words, it hides the exact functionality and schematic of an IC until after the reconfigurable logic has been programmed.

Secure systems designing has been investigated earlier in diverse contexts. Previous works on protection of information systems can be broadly classified into two main categories [1-2]: embedding security mechanisms (access control mechanisms) at various levels of IS; multi-level Kernel-based security architecture.

In the work, the concept of multi-level kernel-based security architecture is considered.

Hardware obfuscation is a technique by which the description or the structure of electronic hardware is modified to intentionally conceal its functionality, which makes it significantly more difficult to piracy. In other words, hardware obfuscation modifies the design in such a way that the resulting architecture becomes unobvious to an adversary [3].

In this work reconfigurable logic-based obfuscation technique exploits reconfiguration features to obfuscate a design [4]. It suggests making a small component of the design reconfigurable in the IC. This approach hides the functional and/or schematic details in untrusted stages of the development cycle.

II. REFERENCE MONITOR OBFUSCATION

A basic concept in the design and development of secure systems is the concept of a reference monitor (RM) – reference validation mechanism.

A RM is an access control concept of an abstract machine that mediates all accesses to objects by subjects [5]. The RM allows developers to integrate the security aspect closer into design process of the system instead of trying to add it later.

The work is devoted to the RM obfuscation, ensuring the key property of RM: the RM must be non-bypassable.

In [6] the authors demonstrate formal transformations of the system structure model using multilevel aggregation. In this work we apply formal transformations approach for the RM obfuscation.

A complex system S is divided into the subsystems S_μ, where $\mu = 1, 2,..., M$. It is obvious that the subsystem S_μ, on the one hand, can itself be a complex system, just like the system S, and on the other hand, it can be an element of the system S.

The system under consideration S consists of 13 elements. The aggregation of the system is realized as follows: $S_\mu=\{C_1,C_2\}$ and $S_{\mu 0}=C_0{}^\mu=\{C_0,C_3 - C_{12}\}$. We assume that the subsystem S_μ will perform the access control functions, in other words, it will be the RM of the system.

The considered obfuscation method of RM consists of two steps. First step consists in construction of the operators (R_μ and $R_{\mu 0}$) of elements connections for the subsystem S_μ and $S_{\mu 0}$. The operator R_μ contains information associated with the connectivity of the RM (S_μ) and the main design ($S_{\mu 0}$). The second step consists in utilization of R_μ for reprogramming the subsystem S_μ at later stages of the design. Practically, we hide the functionality and schematic details of RM.

Proposed method of secure system design involves the access control mechanism as an obligatory element; the obfuscation of RM ensures the nonbypassable property of the access control mechanism; the formalism used in the work allows to automate a secure system design and mathematical

modeling to evaluating its resistance against various forms of attacks.

III. PHYSICAL IMPLEMENTATION

The application of the reconfigurable-based obfuscation of RM for SoC is as follows. The idea of utilization of R_μ for reprogramming the subsystem S_μ at later stages of the design is implemented of in the frame of FPGA platform. The work illustrates the use of reconfigurable feature of the Xilinx Vivado Design Suite and Nexys4-DDR board for obfuscate RM of SoC.

IV. CONCLUSION

In this paper, we have presented the approach that incorporate hardware design obfuscation to protect a design against various forms of attacks. The reference monitor obfuscation is performed using the multilevel aggregation algorithm of the structural model transformation. In order to obfuscate a reference monitor, our approach requires runtime field-programmable hardware features.

REFERENCES

[1] M. Bishop, Computer Security: art and science, Addison Wesley, ISBN 0-201-44099-7, 2002.

[2] C. Pfleeger, S. Pfleeger and J. Margulies, Security in Computing, Fifth Edition, Prentice Hall, pp. 1043, 2015.

[3] A. Sengupta, D. Roy, S. Mohanty and P. Corcoran, "DSP design protection in CE through algorithmic transformation based structural obfuscation," IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 467–476, 2017.

[4] D. Forte, S. Bhunia and M. M. Tehranipoor, Hardware Protection through Obfuscation, Springer International Publishing, 2017 (Chapter 2, Fareena Saqib and Jim Plusquellic, VLSI Test and Hardware Security Background for Hardware Obfuscation).

[5] J. Anderson, "Computer Security Technology Planning Study," Technical Report ESD-TR-73–51, Electronic Systems Division, Hanscom Air Force Base, Hanscom, MA, 1974.

[6] V. Gorbachov, D. Sytnikov, O. Ryabov, A. K. Batiaa and O. Ponomarenko, "Dimension Reduction for Network Systems Using Structure Model Aggregation," International Journal of Design & Nature and Ecodynamics, vol. 15, no. 1, pp. 13–23, February 2020.