Silicon scanning reveals hidden backdoors in semiconductor chips

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

Sergei Skorobogatov

Introduction

With the globalisation of semiconductor manufacturing, integrated circuits become vulnerable to malevolent activities in the form of Trojan and backdoor insertion. An adversary can introduce Trojans into the design during fabrication stage by modifying the mask at a chip foundry. It can also be present inside third parties' modules or blocks used in the design. Backdoors could be implemented by malicious insiders at the design house. Having a security related backdoor on a silicon chip jeopardises any efforts of adding software level protection. This is because an attacker can use the underlying hardware to circumvent the software countermeasures. If a bug is found in firmware programmed into an FPGA then it can be rectified by a firmware update. However, if the Trojan or backdoor is present in the silicon itself, then there is no way to remove the bugs other than replacing all the affected silicon chips and the cost of such an operation is enormous.

The majority of chip manufacturers use the JTAG test interface as a standard port for IC testing. The original specification was expanded in early 2000s with programming abilities and security features to meet the FPGA market demands. It was important for manufacturers to use undocumented commands for granting access to the interface, because in some chips it provided access to the internal memory, usually holding the end user IP and secret data. JTAG, debug port or factory test interface can all potentially be used for scanning.

The JTAG interface is operated via test access port (TAP) pins which control the state machine (Fig. 1). It has two registers – IR (instruction register) and DR (data register) into which the serial data can be shifted and then executed. The IR registers is selected first and then the DR data can be shifted in.

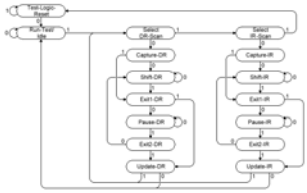

Fig.1. JTAG TAP state machine

Experimental results

We demonstrated how a deliberately inserted backdoor and additional functionalities can be found in the 'highly secure' Actel/Microsemi ProASIC3 Flash FPGA (field-programmable gate array) chip used in both military and sensitive industrial applications.

The JTAG command field was initially scanned for any previously unknown commands by checking the length of the associated DR register (Fig. 2). Some registers were impossible to update with a new data (Fig. 3). All those hidden and non-updatable registers were found to be imprinted into certain locations in FROW memory which is a part of internal Factory settings. As we discovered later, the backdoor allowed writing to all these registers.

We used our own hardware setup for running experiments (Fig. 4). The outstanding sensitivity and performance of our pipeline emission analysis (PEA) method is owed to many factors. One of which is the narrower bandwidth of the analysed signal, another is the low latency that allows real-time analysis. Initially we analysed all the active JTAG commands using power analysis. Fig. 5 shows how AES authentication and Passkey verification traces look, while Fig. 6 shows traces of Array verification and Flash FROM reading commands. That way we were able to find the hidden commands used for backdoor access. Then we used PEA to extract the encryption and access keys to activate the backdoor (Fig. 7).

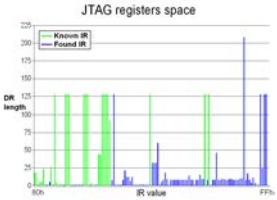

Fig.2. Hidden JTAG DR registers

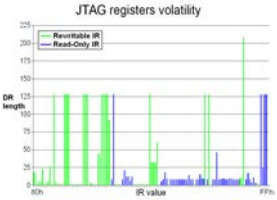

Fig.3. JTAG non-volatile DR registers

Table 1. Security protection levels in ProASIC3 FPGA

Secure Area	Read Access	Verify Access	Write Access	Secure Lock	AES Encryption	Expected Security	Real World Security
FROM (Flash)	Yes	Yes	Yes	Yes	Yes	Days	Seconds
FPGA Array	No	Yes	Yes	Yes	Yes	Years	Days
AES Key	No	Yes	Yes	Yes	No	Days	Seconds
Passkey	No	Yes	Yes	Yes	No	Decades	Hours
Permanent Lock	No	No	Yes	No	No	Centuries	Minutes

Alongside this backdoor there is another layer of security in the guise of data permutation to obscure information and make IP extraction less feasible. This can also be dealt with using a simple brute force attack, because permutation functions do not withstand differential cryptanalysis.

Further investigation of the backdoor key operation revealed that it unlocks many of the undocumented functions, including reprogramming of secure memory areas and IP access. There are some other hidden JTAG functions which give low-level control over the internal shadow memories and allow modification of hidden registers. Our experiments showed how some information can be found via systematic testing of device operations. The simplified outlook of the ProASIC3 security is presented in Fig. 8.

Table 1 summarises the security protection levels in the ProASIC3 devices according to our research findings. All security protection levels fall below expectations by not withstanding low-cost non-invasive attacks as we demonstrated.

To our knowledge, this is the first documented case of finding a backdoor inserted in a real world chip. Most silicon chips are now designed and made abroad by third parties. Is there any independent way to evaluate these products that are used in critical systems?

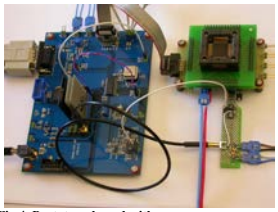

Fig.4. Prototype board with sensor

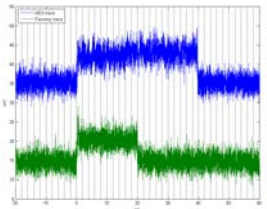

Fig.5. AES vs Passkey JTAG power traces

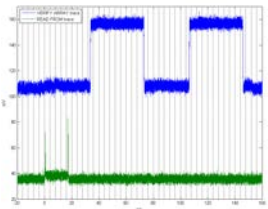

Fig. 6. Array vs FROM power traces

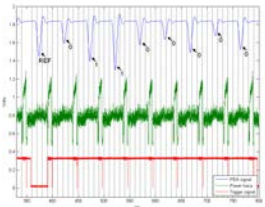

Fig.7. Scanning for keys

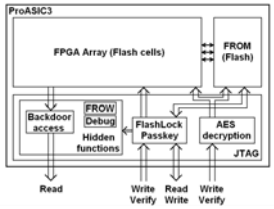

Fig.8. Simplified ProASIC3 security

S. Skorobogatov, C. Woods: Breakthrough silicon scanning discovers backdoor in military chip. CHES Workshop, Leuven, Belgium, LNCS 7428, Springer, 2012, ISBN 978-3-642-33026-1, pp 23–40 *www.cl.cam.ac.uk/~sps32/*

2013-03-22