QUOVADISLABS

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

Researchers' response: Microsemi: Security claims with respect to ProASIC3 May 31, 2012

It was not our intention to make public disclosure at this time as the final paper "Breakthrough silicon scanning discovers backdoor in military chip" was due at CHES workshop in September 2012, where full details of our research will be presented. However, someone other than us posted the news by pointing to our very early drafts of the papers. As a result we had to release the current drafts of our papers so that people could verify our claims.

We have contacted Actel many times about their security issues. This dates back to 2002 when they were warned about a vulnerability in their previous ProASIC devices to glitching and optical fault injection attacks discovered by Sergei Skorobogatov in 2001. In the following years Actel was warned about data remanence, side-channel attacks and optical fault attacks on their ProASIC3 devices. In January 2011 they were warned about Pipeline Emission Analysis (PEA) technique and the security problems we had discovered. We do not know why Actel did not follow up on the concerns we had raised.

Our findings are true for all Actel/Microsemi 3rd generation Flash FPGAs/SOCs including ProASIC3, Igloo, Fusion and SmartFusion. These devices have two official security keys – AES and FlashLock Passcode (passkey) and an undocumented backdoor key which paves the way to access any undocumented security features inside the devices. AES key could help in extracting the embedded intellectual property (IP) but only with some restrictions. The passcode grants Flash memory access and reprogramming of the AES key. The backdoor key opens up readback of the configuration bitstream and other features. The AES key can be extracted with DPA attacks within minutes and with PEA in less than a second. The Passcode key would take years to extract with DPA attack methods, but PEA can extract it within hours.

We used power analysis to find the backdoor in the proprietary JTAG interface of ProASIC3 chip and we used our own PEA technique to understand its functionality. The backdoor allows the readback of all design features including ARRAY, FROM and NVM. This was despite the strong claim made by Actel that such a readback feature was not physically implemented, thus making their devices one of the most secure in the industry. What we found is a backdoor as it falls entirely into the definition given by the dictionary: "Backdoor – an undocumented way to get access to a computer system or the data it contains".

The backdoor feature was designed as a part of the JTAG security protection mechanism and traces can be found in the Actel's Libero FPGA design software. Anyone with this free software installed on their Microsoft Windows machine can go to the Search option in the Start menu and search for one of the fuse names taken from Actel generated STAPL file. For example, search for the word ULUWE in all files. This will return all STAPL files together with templates and algorithm description files. Inside some of those files there is a proof of the designed backdoor feature.

In order to gain access to the backdoor and other features a special key is required. This key has very robust DPA protection, in fact, one of the best silicon-level protections we have ever encountered. With our breakthrough PEA technique we extracted the key in one day and we found that the key is the same in all ProASIC3, Igloo, Fusion and SmartFusion FPGAs. Customers have an option to program their chosen passcode to increase the security; however, Actel/Microsemi does not tell its customers that a special fuse must be programmed in order to get the backdoor protected with both the passcode and backdoor keys. At the same time, the passcode key can be extracted with our PEA technique which is public and covered in our patent so everyone can independently verify our claims. That means that given physical access to the device an attacker can extract all the embedded IP within hours.

There is an option for the highest level of security settings – Permanent Lock. However, if the AES reprogramming option is left it still exposes the device to IP stealing. If not, the Permanent Lock itself is vulnerable to fault attacks and can be disabled opening up the path to the backdoor access as before, but without the need for any passcode.

Sergei Skorobogatov and Christopher Woods, 01 June 2012