Microsemi ProASIC®3 FPGA Security Overview – Update Sept 5th, 2012

A team of academic researchers are presenting a paper at CHES 2012 indicating they extracted a security key in Microsemi's ProASIC®3 FPGAs and several related programmable logic families using a new form of differential power analysis (DPA). Associated with a leaked draft of this paper, a significant amount of media hype was generated that obscured the facts and raised unnecessary alarms.

Facts:

- A new technique of differential power analysis (DPA) was developed that puts all FPGAs and security devices at risk from accelerated DPA techniques, not just those from Microsemi
- These techniques were demonstrated on Microsemi FPGAs because according to the researcher *"This key has very robust DPA protection, in fact, one of the best silicon-level protections we have ever encountered".* FPGAs from other vendors have been broken by older DPA technology since 2011.
- These new techniques require direct access to the Microsemi FPGA device and use custom designed and fabricated test circuits and laboratory equipment
- The researchers identified a "Factory Key" (passcode) that was designed-in by Microsemi for production and failure analysis use
- The alarmist press reports that some third party may have inserted any sort of hidden "back door" into Microsemi devices are false
- The device is protected by the User Passcode (also known as the Flashlock® Passcode or Pass Key), which cannot be bypassed by the Factory Key
- Additional security settings can be employed to block the User Passcode and/or the Factory Key
- Microsemi's next generation FPGA offerings provide a major step forward in security that provides the best mitigation from these type of attacks of any FPGA in the industry

Microsemi has contacted the researchers and reviewed their technology and their findings. The new DPA techniques that were developed by these researchers significantly increase the sensitivity of DPA and put all security devices at much higher risk.

Microsemi is proactively responding to customer concerns raised by the alarmist press. After full reviews of our device security capabilities with customers and the implementation options the customer has chosen, our customers have in general identified that these new techniques have no significant impact on their system security or reliability. Microsemi has also provided additional techniques that significantly increase the security of customer systems where required.

The next generation of highly-integrated FPGAs being introduced this fall by Microsemi utilizes advanced security technology to mitigate these types of security attacks and represent a major evolution in secure FPGA technology.

If you need more information regarding ProASIC3 security or want to learn about the latest security technology, please contact Microsemi security specialist at TechnicalSupport@Microsemi.com.