

Offline Hardware/Software Authentication for Reconfigurable Platforms*

Eric Simpson

Patrick Schaumont, Virginia Tech Secure Embedded Systems Group

As semiconductor capacity continues to grow, designers are developing larger and more complex systems than ever before. To cope with the increasing design complexity, many systems rely on third-party components in their designs. Traditional methods for protecting reconfigurable designs, such as bitstream encryption, are inadequate once third-party components are integrated into the system. Due to the lucrative market for piracy, these third-party components represent valuable intellectual property (IP) that merits protection. In order to protect system developers from counterfeit components, and prevent piracy of the IP providers components, components, a multi-level authentication scheme is necessary. At one level, system developers would like to authenticate the components they are running, and at another level the component providers would like to authenticate the system into which they are integrated.

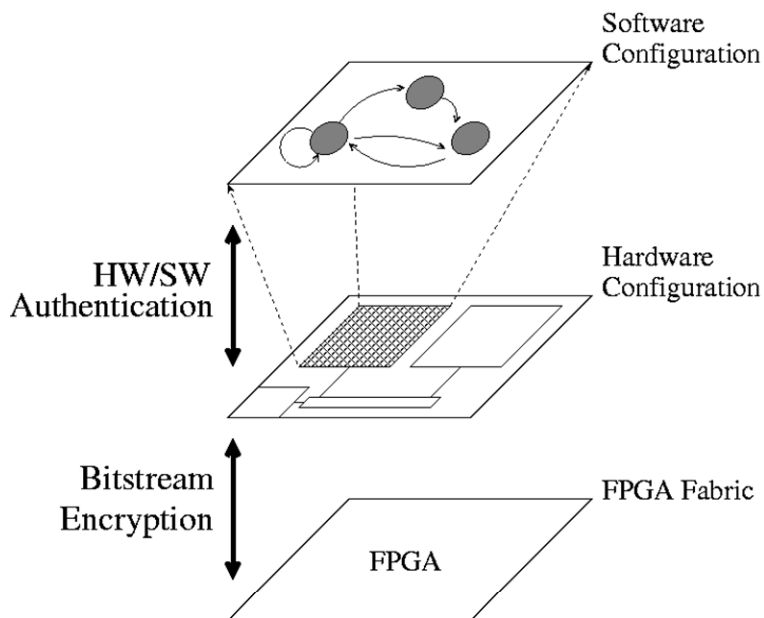


Figure 1. Multiple Layers of Security

We present a solution to the above problems in the form of a protocol and an architectural extension for FPGA-based design. The solution involves the FPGA chip manufacturers, who provide a standard security module in each of their FPGAs, and the component providers, who commit to an identity for each release of their software. An FPGA system developer is then able to combine the chips and third-party components into their product. Using the hardware identity provided by the chip manufacturers and software identity committed to by the component providers, they are able to construct a product where hardware and software components can authenticate each other, thereby solving the multi-level authentication problem. Our solution to hardware, software authentication is lighter weight than the Trusted Computing Platform (TPM) approach, and seamlessly integrates with the existing FPGA design flow. We are able to demonstrate an implementation of the authentication scheme that only requires a symmetric cipher and a Physically Unclonable Function (PUF). In addition to the low hardware requirements, our implementation does not require any on-chip, non-volatile storage.

* Conducted as an undergraduate research project in the Secure Embedded Systems Group in the ECE department. Accepted for publication in the Workshop on Cryptographic Hardware and Embedded Systems 2006 (CHES 06), Yokohama, Japan, October 2006.