Overview of Design Security Using Microsemi FPGAs and SoC FPGAs

November 2013

Introduction

The security of electronic systems can be divided into two major classes: Design Security and Data Security. The goal of Design Security is to ensure that the owner's hard work and valuable Intellectual Property (IP) are protected and intact at all times. Data Security refers to applications that a system utilizes to protect and authenticate data. Typical examples of Design Security would be protecting the contents of the FPGA configuration bitstream from ‘snooping’, copying, or reverse engineering. If the configuration bitstream can be copied a competitor can simply ‘clone’ boards with the same function and sell them at a much lower cost, since they have no cost associated with developing the product. Even worse, an unscrupulous contract manufacturer could build additional units and compete with their customer!

This overview will introduce several key Data Security concepts that are helpful in understanding the advanced features available in SmartFusion®2 and IGLOO®2 for implementing Design Security functions in embedded system designs. If you are unfamiliar with some of the security terms used in this paper it may be helpful to refer to the Online Security Glossary hosted on the Microsemi Security website. A link to the Glossary is given in the "To Learn More" section at the end of this paper.

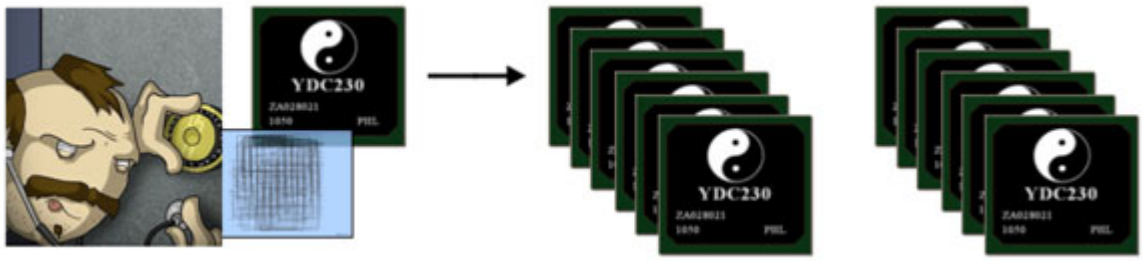

Figure 1: **Two Common Design IP Threats are Reverse Engineering and Overbuilding**

Threats to Your Design

The best starting point for understanding Design Security is to identify the most common threats to your design, and in particular the threats to the valuable Intellectual Property (IP) incorporated in your design. After spending significant effort and funds constructing a leading edge embedded system you certainly don't want a competitor or unscrupulous contract manufacturer to be able to benefit from your hard work. Four of the most common threats you may face are: Over-building, Cloning, Reverse Engineering, and Denial of Service.

Over-Building

Over-building is by far the most common security attack that takes place. The increasing reliance on using standard off the shelf products during embedded systems design makes it easy for unscrupulous manufacturers to over-build with. In addition to the inventory required to make systems as contracted by the embedded systems design house, it is common for additional unauthorized systems to be built with the inventory of standard parts (for example, FPGAs, Microprocessors, and Memory) bought on the open market. The contract manufacturer has all the ingredients necessary to build a product! The unauthorized over built inventory, which is identical to the genuine product, is sold for profit with none of the support and design overhead associated with developing the product.

Cloning

While over-building is a more prevalent and opportunistic crime, both cloning and reverse engineering are serious problems too. In cloning, a competitor makes a copy of a design by stealing part or all of the system's Intellectual Property (IP). This is accomplished by copying the FPGA and/or microcontroller boot code.

The single point of failure or the weak link in systems that can easily be cloned, are nonvolatile memories used to store configuration data for FPGAs and/or microprocessors. Unless strong security schemes are used, even devices with security 'bits' can easily be copied. There are several companies that specialize in copying CPLDs, flash MCUs, and similar logic products.

Reverse Engineering

In reverse engineering a competitor will not only extract the raw data from a device (as in cloned systems), but will also reverse engineer the programming code to extract explicit details on how the design works. This may be done by disassembling microcontroller codes and reconstructing assembly code from the raw hex file or from the photographic analysis of an ASIC layout, as each layer is removed and analyzed for functionality. Reverse engineering techniques will give a competitor all of the IP used in a design and allow them to reuse it, improve on it, and easily disguise it to thwart possible legal action.

Denial of Service

While Denial of Service (DoS) is not a theft technique, the consequences can be more damaging and easily preventable with secure embedded solutions. DoS attacks use in-system programming techniques to render the logic of an FPGA or the code of a microcontroller inoperable by configuring them to run 'bad code'. Distributed Denial of Service (DDoS) attacks have crippled several high-profile websites over the past several years using software techniques. Any unsecured in-system programmable device is a potential target for DoS attack, whether it is an SRAM FPGA, ISP CPLD, or flash-based microcontroller running in a critical part of a network/telecom system. The recent introduction of tools for finding unsecured embedded systems (like Shodan, the home page of which is depicted in Figure 2) show that over 500 million internet control systems (such as web cams, routers, and power plants) could be at risk (according to advice given recently to the U.S. Department of Homeland in the “ICS-CERT Alert Oct 25, 2012” Security Report, see the "To Learn More" section of this paper for the link to the Report).

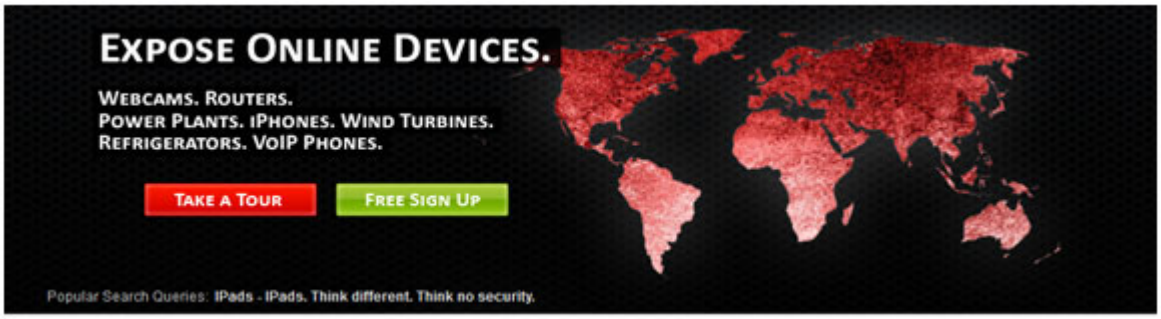

Figure 2: **The Use of Online Tools Like Shodan Uncover Unsecured Embedded Systems**

Making matters even worse, commercially available tools for testing your own networks vulnerabilities can be used in conjunction with Shodan to penetrate embedded systems. There are also open source projects leveraging Shodan’s capabilities to automate and ‘test’ thousands of embedded systems at a time, recording those with known weakness.

Using Microsemi FPGAs to Protect Your Design from Security Threats

Microsemi FPGAs and SoC FPGAs have been designed from the ‘ground up’ to provide the most robust platform for creating secure designs. Starting with an inherently secure flash technology, Microsemi adds a wide range of security features that can be used to address each of the common threats to your design. These capabilities are described below.

Protection Against Over-Building

Preventing cloning of devices can dramatically reduce the incidence of overbuilding of systems by unscrupulous contract manufacturers or rogue insiders since the number of properly programmed devices can be tightly controlled. All Microsemi flash-based devices have several security features that are available to prevent cloning and the newest SmartFusion2 and IGLOO2 devices have several new security features for even more robust security capabilities.

FlashLock Technology with 256-Bit Passcode

Microsemi flash-based FPGAs include FlashLock® technology to lock the device with a 256-bit passcode, which allows the device to be unlocked and reprogrammed by providing the same passcode. Passcodes are initially programmed in encrypted form, and when re-entered to unlock the device they may be also be encrypted, facilitating their use in less-trusted locations. In addition, a permanent lock is possible, which disables all programming access to the part, turning them into One Time Programmable (OTP) devices and thus very secure from attempts to subvert the function of the target design.

Program In-House Before Sending to the Contract Manufacturer

Microsemi flash FPGAs can be programmed in-house with a user supplied AES key, then shipped to a contract manufacturer for final programming. The contract manufacturer programs the device with the AES-encrypted bitstream, hence only devices with the same AES decryption key will get programmed. Microsemi can provide trusted in-house programming services for just keys or for entire device configurations, if desired. Microsemi makes it easy to create a secure manufacturing flow, illustrated in Figure 3 below, through the Libero® design tools. Within the Libero tool, the designer simply creates a security settings file along with an associated encrypted bitstream file. In this case, the keys are sent to Microsemi or a distributor and programmed with the desired security keys. The keyed devices are sent to the contract manufacturer and programmed with the associated encrypted bitstream files safely and securely.

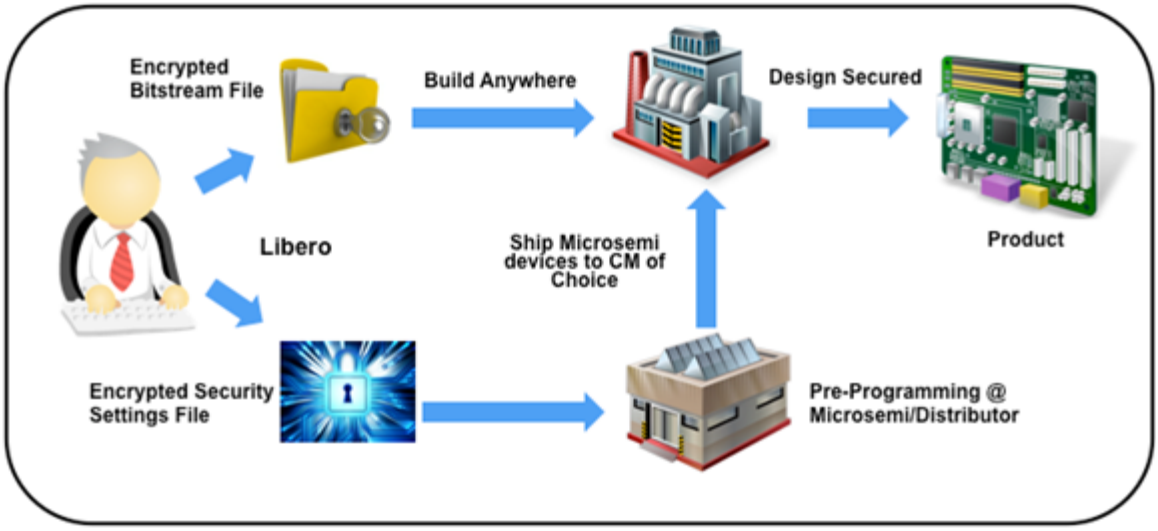

Figure 3: **Secure Manufacturing Flow**

Drop-Ship Devices Directly to the Contract Manufacturer

Since even the initial injection of user bitstream keys is done in encrypted form in SmartFusion2 or IGLOO2 devices, all programming configuration steps can be performed in a non-trusted manufacturing environment, thus eliminating requirements for an expensive trusted facility or the need to physically transfer devices between trusted and normal manufacturing locations. No longer do keys appear in plaintext or protected only by weak obfuscation techniques. The capability to load user keys using strong cryptography and best-in-class key management practices at every step are unique to SmartFusion2 and IGLOO2 devices, across the entire FPGA industry. SmartFusion2 and IGLOO2 FPGAs make strong security easy to implement.

Protection Against Reverse Engineering

A number of factors complicate attempts to compromise a Microsemi flash FPGA or SoC FPGA. Because all programming is done securely, the attacker is left with attempting physical attacks on the device to try and determine the contents of the configuration bitstream. In order to determine the state of any given flash element, the microscopic size and sheer number of the switches make it essentially impossible to locate each cell and identify its programming state. Invasive probing to evaluate each flash switch would result in the destruction (flash cell charge removal) of the very programmed states needed to reverse engineer the design. Even if the bitstream could be extracted, reverse engineering the bitstream to a meaningful schematic can be an extremely tedious and error-prone process.

The SmartFusion2 FPGA provides additional protections against reverse engineering. For example, bitstream keys are stored on-chip in encrypted form, and passcodes are cryptographically hashed. Differential power analysis (DPA) countermeasures are applied to prevent extraction of keys during use. All protocols have been hardened against tampering. Countermeasures are even provided to prevent or at least detect many semi-invasive or invasive attacks, such as tampering with security settings with lasers or probes, whereupon the device can be commanded to destroy all sensitive data before it can be compromised through the zeroization system service

Protection Against Denial of Service (DoS)

While flash FPGAs can be in-system programmed (ISP), if desired, they can also prevent DoS attacks by only allowing ISP to key holders or by disabling the ISP capability completely (lock permanently). Flash FPGAs and SoC FPGAs can also be programmed with AES encrypted bitstream, allowing only authorized and validated bitstreams to be programmed to the device.

SmartFusion2 and IGLOO2 FPGAs only work with encrypted, authenticated bitstreams—no plaintext bitstreams are ever used, and encrypted FlashLock® passcodes can be used to provide another layer of security while still allowing field upgrades in less-secure locations. SmartFusion2 and IGLOO2 devices can be reprogrammed remotely using an AES encrypted programming file for easy and secure field upgrades. Intercepting the encrypted configuration bitstream is useless; an appropriate AES decryption key is required in order for an encrypted configuration bitstream to work. Bitstream files are not only encrypted for confidentiality but also fully authenticated, providing proof of integrity and heritage.

SmartFusion2 and IGLOO2 FPGAs also provide several autonomous programming modes and advanced features like ‘roll-back’ protection, where an adversary tries to use a previous version of a configuration bitstream using previously identified security weaknesses as attack vectors.

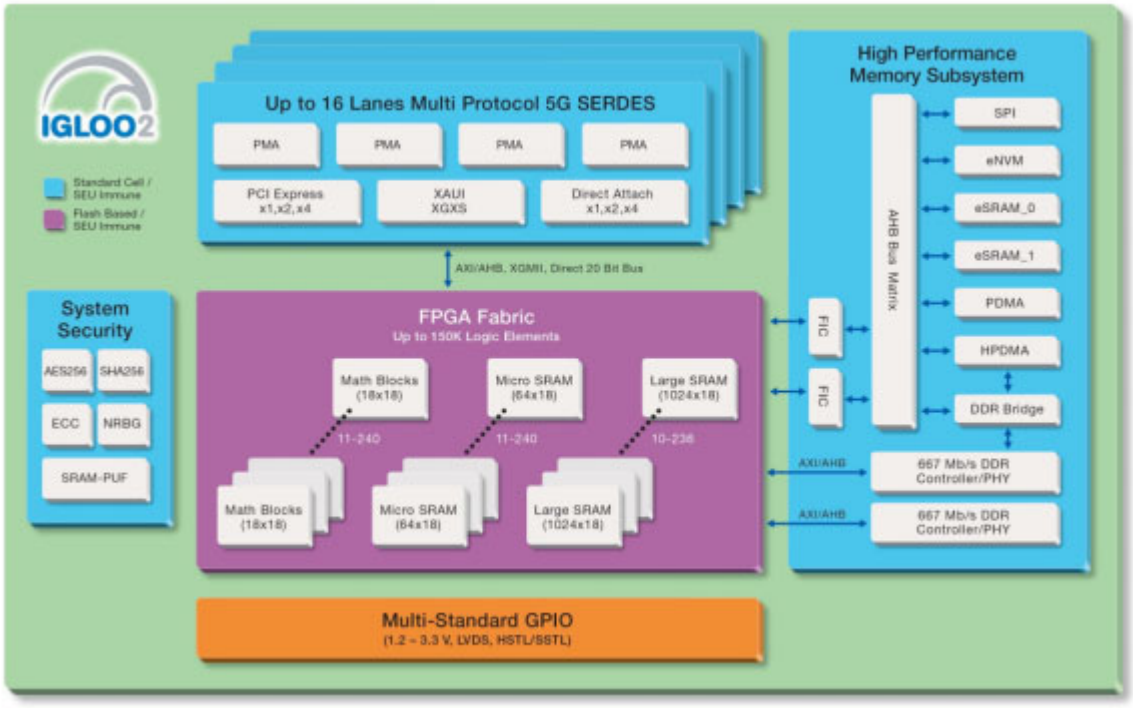

Figure 4: **IGLOO2 Functional Block Diagram Showing the Security System**

SmartFusion2 and IGLOO2 Unique Design Security Capabilities

Below is a list of many of the security features available in SmartFusion2 and IGLOO2 devices. Many of these features are managed and controlled through the ‘hardcoded’ System Security block shown on the left side of Figure 4 (This figure illustrates this block in an IGLOO2 device but a similar block exists in SmartFusion2 devices also). Other security features, such as secure flash configuration bit stream storage within the FPGA fabric, a variety of advanced anti-tamper protections, and the many security settings, passwords, and ‘lock-bits’ are distributed throughout the chip, but work in conjunction with the System Security block to further protect your design from even the most security threats.

- Intellectual Property (IP) Protection
  - All bitstreams always encrypted using AES with 256-bit keys and fully authenticated with a 256-bit tag
  - Protection against device cloning and system-level overbuilding
  - Bitstream validation service (without committing to program device), making for safer upgrades using data which may have been corrupted (accidentally or maliciously) in transit to a system in the field
- Automated Secure Key Management and Programming Modes
  - Encrypted User Key and Bitstreams Loading. Three initial key choices:
    - Default Key-Loading key

        - Unique per-device Factory Key
        - Ephemeral key using public-key (ECC) methods (-100 and -150 only); can use either the Factory ECC key or the PUF ECC key, both of which are certified.
    - Switch over to user keys, once loaded
    - Certificate-of-Conformance to ensure the device was programmed as intended
    - Enables programming in less-trusted locations
- Supply-Chain Assurance
    - Uses X.509 -conforming "Device Certificate" signed (certified) by Microsemi ensuring integrity of signed data and proving the certificate came from Microsemi
    - Binds the part number, serial number, date code, and others to the device secret key(s), assuring their authenticity and their binding to the device
    - Certifies ECC public keys (-100 and -150 only) includes the PUF key, providing exceptionally strong unclonable "biometric" binding to the device
- Zeroization
    - Three active options, plus Zeroization can be disabled
        - Like-new (retains factory keys and serial number); the device can be instantly reprogrammed
        - Recoverable (zeroizes factory keys, but new factory keys and serial number can be injected using authenticated key recovery service)
        - Unrecoverable (zeroizes everything and locks the device)
- Enhanced Anti-Tamper Features
    - Differential Power Analysis (DPA) countermeasures using CRI patented techniques
    - On-Demand Data Integrity Check for all nonvolatile memories to ensure reliability and security against both natural errors and malicious attacks
    - Data Integrity Check is also available as an automatic power-up option
    - Extensive well-monitored redundancy
    - Options to disable debugging features, includes ARM debugging modes (on SmartFusion2 devices), FPGA fabric probes, and JTAG boundary scan
    - Reversible and permanent lock options; 256-bit passcodes used for unlocking may use encrypted replay-protected protocol or plaintext passcode protocol
    - Other passive and active countermeasures
- Advanced features like Variations and Back-Tracking prevention
    - Variations allow a small part of bitstream to be unique-per-device, but still authenticated as part of whole
    - Back-tracking prevents replaying old previously valid bitstreams (also known as downgrading)
- Various information services, such as exporting of the Serial Number, JTAG USERCODE, or Device Certificate
- Key verification protocol to prove the device knows the secret key(s)
    - Symmetric factory secret key using a factory key database
    - Symmetric user secret key(s), knowing the keys that were injected
    - Private half of the factory ECC and PUF ECC Public Key pair(s) using the certified Public Key half

Conclusion

This paper has provided an overview of several of the most important Design Security concepts in the context of implementations using SmartFusion2 and IGLOO2 devices. As you can see, there are many more security features available than we were able to cover in detail in this overview. These concepts should provide the reader with an excellent starting point for digging deeper into the security needs for a specific design.

We hope you are encouraged to find out more about how you can protect your design IP from the threats described in this paper, and any new ones that might show up in the future. Please use the wealth of information we list in the "To Learn More" section below, or by visiting the Microsemi Security website to expand your security knowledge and capabilities.

To Learn More

1. ICS-CERT Alert Oct 25, 2012
2. Securing Your Embedded System Life Cycle
3. Securing Your Supply Chain Life Cycle
4. Protect FPGAs from Power Analysis
5. What is Design Security in a Mainstream SoC Chalk Talk

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.

55900161-0/11.13