Security Scenarios

February 2014

Table of Contents

Introduction

As FPGAs grow in capability through the million-gate mark, they are being used for ever more complex and valuable designs. This trend toward the pervasive use of FPGAs raises questions about embedded design security, a subject that is not always well understood. Using a number of typical cases from various industries, the following scenarios illustrate some common security problems facing today's designers, and possible solutions for preventing future infringements.

Scenarios

The following security scenarios were developed by a third-party expert in the field of security engineering as part of a study funded by Microsemi and represent a wide variety of real world threats that could significantly damage your business.

1. Overbuilding Counterfeit

Red Sound Incorporated makes MP3 players for the USA and Europe. A household brand, Red Sound subcontracts the manufacture of the devices to Lotus Audio in Bangkok. After producing 250,000 units for Red, Lotus makes an additional 100,000 identical units (including not just Red Sound's design but also their own label), which are then sold through grey market importers.

Comment:	Overbuilding fraud is the largest single source of counterfeit goods, and in some sectors, the sole source.
Requirement:	Red Sound needs a mechanism to stop overproduction. Many different industries have incurred this type of problem. For example, in the cosmetics industry, ingredients and packaging are sourced from multiple suppliers whose identities are kept secret from the contract manufacturer. One strategy is to program in-house, and supply only programmed parts to the manufacturers. An alternative method is to use keys (embedded in an auditable quantity of FPGAs supplied by a vendor or trusted third party) that enable Red Sound to lock (and protect) its bitstream.

2. Data Manipulation

Blue Phone Company is a GSM operator in France, where handsets are subsidized by the service providers and sold for a nominal amount to users, provided the customer signs a one-year service contract. The problem occurs when grey market traders buy phones for resale in countries, such as Norway and Singapore, where handsets are not subsidized. This effectively robs both Blue Phone of its subsidies intended for French users, and, in some cases, allows users in foreign markets to obtain unauthorized access to their local mobile networks without paying.

Comment:	Past attempts to prevent grey exports from using handset software have been circumvented by pirates within a few weeks.
Requirement:	Because of the prevalence of subsidies in mobile phone business models, many phone companies want to ensure that the new, expensive WAP and 3G handsets now being introduced be tied firmly to the home network. Handset vendors want to assure the phone companies that handsets will be difficult to reprogram. There is little concern about "knock-off" copies of phones because of the scale economies required to achieve competitive prices, and because of the regulatory environment.

To make the phone secure, it must be made very costly to change a particular variable in the phone, such as the identity of the home network. Typically achieved with secure, serialized, or system-authenticated programmable devices, this solution is similar to another well-studied problem: software protection using dongles.

3. Software Protection

Green Mapping Company sells software to make maps from aerial photographs. Its customers are mostly local governments, buying the systems for $20,000. Approximately half of the cost results from the hardware (scanners and plotters), while the remaining expense is the software. As the price of hardware decreases, Green Mapping has become increasingly anxious about piracy. The company wants to implement a high-quality hardware dongle that must be present for its software to run, which will eliminate security problems.

Comment: Many software companies used dongles in the early 1980s, after which they went out of fashion. They are now reappearing in sectors with high-value products. In 1998, about a million dongles were sold worldwide at an average price of approximately $20.

Requirement: A medium-quality dongle might contain a digital signature mechanism that the program would challenge from time to time. The main threat is that a pirate will patch out the calls to this mechanism. A better solution is to implement some important part of the program logic in the dongle, such as a digital filter, or part of a rendering algorithm. After using this method, a successful attack would necessitate either copying the device completely or understanding its critical functionality.

4. Compatibility Control

Purple Games Incorporated sells a gaming console. Their plan for success employs a business model in which royalties from game sales and accessories subsidize the cost of the consoles. Purple Games has therefore implemented an authentication mechanism for its game cartridges using an FPGA. The company is very anxious to prevent third party vendors from copying its products, or from reverse-engineering it to the extent that they can make compatible cartridges. Purple Games' choice of attack involves utilizing the Digital Millennium Copyright Act (DMCA) very aggressively against unlicensed suppliers.

Comment: Several game companies have used FPGAs due to their fast time-to-market advantage.

Requirement: The requirement is for a tamper-resistant chip that combines copyright control and accessory control functions, while still being difficult to reverse-engineer. Additionally, low design costs are necessary, as some accessory retail prices are less than $10.

5. Product Versioning

Tartan Scientific Instruments sells oscilloscopes and similar test equipment. In its business model, products are versioned according to the amount of high-speed RAM available; academics can buy an oscilloscope with 8 MB of RAM for $4000, while the professional version has 64 MB of RAM and costs $17,000. All products have the same hardware; the difference is that customers paying the professional price get a password that unlocks the extra memory. This mechanism has been defeated, and the password is circulating on the Internet. Tartan wants to use an FPGA to better protect its next model.

Comment:	Product versioning and price discrimination are now the fastest-growing application areas for cryptography and related information security mechanisms.
Requirement:	The FPGA will check the password and also perform some critical signal-processing role. A mechanism whereby it encrypts access to the memory might also be an adequate solution.

6. Secure Reconfiguration

The NSA has been working with several companies to develop prototypes for secure reconfiguration of FPGAs. Rather than having an external device, such as a microcontroller to manage the download of a bitstream, their goal is to have a "security kernel" in one of the chip contexts that can be utilized to authenticate the download of other contexts.

Comment:	Several large consumer-product companies have been investigating this issue.
Requirement:	Given a suitably trustworthy download authentication mechanism, it should not be necessary for FPGA customers to develop their own. The NSA's stated requirement is that the bitstream comes from an authenticated source, that it should not be changed, whether maliciously or inadvertently, and that its confidentiality should be protected.

7. Litigation Risk Avoidance

Orange Appliance Company is producing consumer appliances in professional audio processing, an area troubled with litigation. Orange Appliances wants to keep the signal processing algorithms it uses secret to avoid the costs of being sued by competitors, who might use valueless patents to impede the company.

Comment:	The threat of vexatious litigation was the reason cited by IBM in the 1980s for no longer supplying source code for operating systems, and is a reason cited by Microsoft today.
Requirement:	The requirement is that the cost of reading out and understanding the bitstream should exceed the cost of successfully bringing a lawsuit, or part of a lawsuit, to compel its disclosure.

To Learn More:

Secure Life Cycle

1. Securing Your Embedded System Life Cycle
2. Securing Your Supply Chain Life Cycle

Protecting Your Design IP

1. Protect FPGAs from Power Analysis
2. How Easy is it to Secure Your Designs?
3. What is Design Security in a Mainstream SoC Chalk Talk?