SECURE PARTIAL RECONFIGURATION OF FPGAs

Amir H. Sheikh Zeineddini
Outline

- FPGAs Security
- Proposition
- Implementation
- Experiment Methodology
- Results and Conclusions
FPGAs SECURITY
FPGAs Technologies

- **Volatile**
  - SRAM
    - Truly Reconfigurable
  - Largest Market Share
  - Lowest level of security

- **Non-volatile**
  - Antifuse and Flash
    - Not truly reconfigurable
  - Higher level of Security
SRAM FPGA Configuration

- Loading the bitstream into internal memory by delivering it through one of the configuration interfaces

- Configuration phases:
  1. Clearing the configuration memory
  2. Initialization
  3. Bitstream loading
  4. Device startup
Types of Attacks

- Cloning

- Reverse Engineering

- Tampering

**Countermeasures:**
*Encryption and Authentication*
Major Disadvantages:
- Need of an external battery
- No flexibility
- Partial reconfiguration via the external configuration interfaces is not permitted for encrypted bitstreams.
Algotronix Solution

Initial Programming:

- Non-encrypted Bitstream
- Configuration Device
- Encrypted Bitstream

Configuration Device

Encrypted Bitstream

Configuration Device

Configuration Memory

Secret Key

Normal Configuration:

- Configuration Device
- Encrypted Bitstream
- SRAM FPGA

Configuration Interface

Encryption Circuit

Configuration Logic

Configuration Memory

Secret Key

Solution by Bossuet et al.

- **Major Advantages:**
  - No hard-wired encryption/decryption circuits
  - No additional battery

- **Major Disadvantages:**
  - Not feasible
  - Management of partial reconfiguration
  - Complex system, keys management

PROPOSITION
Desirable Characteristics

- Strong protection against:
  - Cloning
  - Reverse engineering
  - Tampering

- Flexibility
  - Providing the key
  - Choice of a suitable algorithm (security policy)

- Least amount of fixed resources (hard IP)
Our Solution

External Memory

- IP 1 Encrypted
- IP 2 Encrypted
- IP 3

Xilinx FPGA

Configuration Controller

- PowerPC or MicroBlaze
- Processor IP Cores

Application System

- IP 3
- IP 2
- IP 1

---

Image Source: George Mason University
Our Solution (cont.)

- Solution for a secure partial reconfiguration after initial configuration

- Method exploits:
  - Embedded processor cores
  - Dynamic Partial Reconfiguration
  - Software Control

- Scheme provides:
  - Flexibility (arbitrary algorithm for encryption/decryption)
  - NIST approved authentication
IMPLEMENTATION
Virtex-II Pro Architecture

Features:

1. Processor Block
2. RocketIO Multi-Gigabit Transceivers
3. CLB and Configurable Logic
4. SelectIO-Ultra
5. Digital Clock Managers
6. Multipliers and Block SelectRAM

We are interested in:
- Embedded processor core
- Dynamic partial reconfigurability
Processor Block

- Contains four components:
  - Embedded IBM PowerPC 405-D5 RISC CPU core
  - On-Chip Memory (OCM) controllers and interface
  - Clock/control interface logic
  - CPU-FPGA Interfaces

- IBM CoreConnect Bus Architecture Features:
  - Processor Local Bus (PLB)
  - On-chip Peripheral Bus (OPB)
  - Device Control Register (DCR) Bus
Partial Reconfiguration

- Loading only a subset of frames into the FPGA

- Different forms:
  - Static: Rest of the device is in reset (shutdown)
  - Dynamic: Rest of the device remains operational
    - Advantages:
      - Runtime reconfiguration
      - Efficient resource utilization
  - Self-reconfiguration: dynamic reconfiguration + specific circuit on the FPGA to control partial reconfiguration
Xilinx ML310 Evaluation Board

Virtex-II Pro
XC2VP30 FF896

System ACE
256 DDR SDRAM
High Speed PM 1
High Speed PM 2

Compact Flash

RS232
SMBus
SPI EEPROM
GPIO / LEDs

Intel 10/100 Ethernet NIC
TI PCI 2250
5V PCI Slots (2)
3.3V PCI Slots (2)

RJ45
3.3V PCI

AMD Flash
GPIO
IDE (2)

ALi M1535D+ South Bridge
USB (2)
Audio
SMBus

RS232 (2)
PS/2 K/M
Parallel Port
Design Tools

- Xilinx Embedded Development Kit (EDK)

- Xilinx ISE Foundation design environment

- Software Libraries:
  - AES encryption / decryption algorithm
  - HMAC-SHA1 authentication algorithm
    (Both implemented by Dr. B. Gladman)
EDK Tools Flow

**Hardware Flow**
- Processor IP MPD Files
- VHDL / Verilog
  - PlatGen
  - Synthesizer
    - Microprocessor Hardware Specification File
    - EDIF IP Netlists
      - ISE / Xflow
        - System Constraint File
        - Bitstream
          - Data2MEM
            - Download to FPGA

**Software Flow**
- C / C++ Code
  - Compiler
  - Object Files
  - Linker
    - Executable
  - Libraries
    - Microprocessor Software Specification File

---

**Libraries**

---
PowerPC System

PLB = Processor Local Bus
OPB = On-chip Peripheral Bus
ICAP = Internal Configuration Access Port
HWICAP = Hardware ICAP
XMD = Xilinx Microprocessor Debugger
Hardware Internal Configuration Access Port (HWICAP)

- Hardware ICAP (HWICAP) is used for:
  - Configuration read/write
  - Loading partial bitstreams

- ICAP:
  - Subset of SelectMAP interface
  - Located in the lower right corner of the device
MicroBlaze System

- ILMB = Instruction-side Local Memory Bus
- DLMB = Data-side Local Memory Bus
- OPB = On-chip Peripheral Bus
- OPB Wd Timer = OPB Watchdog Timer
- ICAP = Internal Configuration Access Port
- HWICAP = Hardware ICAP
- XMD = Xilinx Microprocessor Debugger
EXPERIMENT METHODOLOGY
Xilinx Partial Reconfiguration Styles

Extent of Partial Reconfiguration

Small
Difference-based
Front-end Modification (HDL Entry, Synthesis, Implementation)
Modified Design '.ncd' file
BitGen generates a partial bitstream

Large
Module-based
Design Entry HDL Entry/Synthesis
Initial Budgeting
Active Module Implementation (Map, Place, Route)
Top-level
Final Assembly (Map, Place, Route)

Back-end Modification (Using FPGA Editor)
Initial Design Bitstream
Module-based Flow (cont.)
# Module-based Flow Evaluation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level of required effort</strong></td>
<td>High; needs more than average acquaintance with the tool</td>
</tr>
<tr>
<td><strong>Level of support of existing tools</strong></td>
<td>Problematic with frequent errors especially for complex designs</td>
</tr>
<tr>
<td><strong>Practical limitations</strong></td>
<td>Requires:</td>
</tr>
<tr>
<td></td>
<td>- A full design for initial reconfiguration</td>
</tr>
<tr>
<td></td>
<td>- Special consideration for inter-module communications</td>
</tr>
<tr>
<td></td>
<td>- Different constraints for modules</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>Automation and bounded routing</td>
</tr>
</tbody>
</table>
Difference-based Flow

Virtex-II Pro

User Interface

ML310 LEDs

XMD

JTAG Interface

GPIO

OPB

DOPB

MicroBlaze
CPU Core

ILMB

DLMB

Dual-ported
BRAM

8K of BRAM
partially reconfigured
in MicroBlaze system area

PowerPC / MicroBlaze
Self-reconfigurable platform area
(IPs not shown)

PowerPC
or MicroBlaze

ML310 DDR SDRAM

Static Area

Reconfigurable Area
Difference-based Flow (cont.)
## Difference-based Flow Evaluation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level of required</strong></td>
<td>Medium depending on the changes made and level of acquaintance with the tool</td>
</tr>
<tr>
<td><strong>effort</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Level of support of existing tools</strong></td>
<td>Acceptable with occasional errors and problems</td>
</tr>
<tr>
<td><strong>Practical limitations</strong></td>
<td>Not recommended if routing changes is desired</td>
</tr>
<tr>
<td><strong>Benefits</strong></td>
<td>Small partial bitstreams (Multiple-frame Write)</td>
</tr>
</tbody>
</table>
RESULTS AND CONCLUSIONS
Timing Measurement Method

- Phases of the program running on the processor core of the configuration controller:

  - Authentication
  - Decryption
  - Configuration

  10 measurements 10 measurements 10 measurements
Timing Results I

- **Difference-based Flow:**
  - 10 measurements for each phase (clock cycles)

- **PowerPC system:** no extra component (time-base register)

- **MicroBlaze system:** OPB Watchdog Timer

- **Size of partial bitstream:** 14112 bytes

<table>
<thead>
<tr>
<th>Phase</th>
<th>PowerPC System</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication</td>
<td>Decryption</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>13,862,435</td>
<td>20,838,769</td>
<td>5,630,038</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>13,862,591</td>
<td>20,838,876</td>
<td>5,631,061</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>13,862,486</td>
<td>20,838,769</td>
<td>5,630,038</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>13,862,435</td>
<td>20,838,769</td>
<td>5,630,038</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>13,862,500</td>
<td>20,838,769</td>
<td>5,631,037</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>13,862,575</td>
<td>20,838,776</td>
<td>5,630,038</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>13,862,591</td>
<td>20,838,876</td>
<td>5,628,993</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>13,862,575</td>
<td>20,838,776</td>
<td>5,630,038</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>13,862,591</td>
<td>20,838,879</td>
<td>5,628,993</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>13,862,486</td>
<td>20,838,769</td>
<td>5,631,037</td>
<td></td>
</tr>
<tr>
<td>Std. Dev.</td>
<td>65</td>
<td>51</td>
<td>756</td>
<td></td>
</tr>
<tr>
<td>Mean</td>
<td>13,862,527</td>
<td>20,838,803</td>
<td>5,630,131</td>
<td></td>
</tr>
<tr>
<td>% Error</td>
<td>0.05%</td>
<td>0.02%</td>
<td>1.34%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase</th>
<th>MicroBlaze System</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Authentication</td>
<td>Decryption</td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>77,649,436</td>
<td>147,201,543</td>
<td>3,175,996</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>77,649,453</td>
<td>147,201,601</td>
<td>3,175,964</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>77,649,510</td>
<td>147,201,675</td>
<td>3,175,420</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>77,649,416</td>
<td>147,201,543</td>
<td>3,175,996</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>77,649,510</td>
<td>147,201,675</td>
<td>3,175,943</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>77,649,349</td>
<td>147,201,675</td>
<td>3,175,996</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>77,649,597</td>
<td>147,201,639</td>
<td>3,175,996</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>77,649,597</td>
<td>147,201,675</td>
<td>3,175,952</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>77,649,515</td>
<td>147,201,451</td>
<td>3,175,008</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>77,648,899</td>
<td>147,201,639</td>
<td>3,175,996</td>
<td></td>
</tr>
<tr>
<td>Std. Dev.</td>
<td>201</td>
<td>77</td>
<td>179</td>
<td></td>
</tr>
<tr>
<td>Mean</td>
<td>77,649,428</td>
<td>147,201,612</td>
<td>3,175,927</td>
<td></td>
</tr>
<tr>
<td>% Error</td>
<td>0.03%</td>
<td>0.01%</td>
<td>0.56%</td>
<td></td>
</tr>
</tbody>
</table>
Timing Results II

<table>
<thead>
<tr>
<th>System</th>
<th>Authentication</th>
<th>Decryption</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ave. Time (ms)</td>
<td>PowerPC 139</td>
<td>208</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>MicroBlaze 776</td>
<td>1472</td>
<td>32</td>
</tr>
<tr>
<td>Throughput (KB/s)</td>
<td>PowerPC 102</td>
<td>68</td>
<td>251</td>
</tr>
<tr>
<td></td>
<td>MicroBlaze 18</td>
<td>10</td>
<td>444</td>
</tr>
<tr>
<td>Ratio</td>
<td>PPC / MB 5.6</td>
<td>7.0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System</th>
<th>Clock Cycles / Byte</th>
<th>Clock Cycles / 16 Bytes Block</th>
<th>Clock Cycles / 4 Bytes Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerPC</td>
<td>982</td>
<td>23,627</td>
<td>1,596</td>
</tr>
<tr>
<td>MicroBlaze</td>
<td>5,502</td>
<td>166,895</td>
<td>900</td>
</tr>
</tbody>
</table>

- Comparison of the timing results for each phase
  - PowerPC
    - Faster authentication and decryption time
    - Slower configuration time
  - Throughput is not the major concern but area
Device Utilization Summary

PowerPC System
- Number of MULT18X18s: 0 out of 136 (0%)
- Number of RAMB16s: 5 out of 136 (3%)
- Number of SLICEs: 1334 out of 13696 (9%)
- Number of PPC405s: 1 out of 2 (50%)
- Number of BUFGMUXs: 7 out of 16 (43%)
- Number of DCMs: 2 out of 8 (25%)
- Number of JTAGPPCs: 1 out of 1 (100%)
- Number of ICAPs: 1 out of 1 (100%)

MicroBlaze System
- Number of MULT18X18s: 3 out of 136 (2%)
- Number of RAMB16s: 5 out of 136 (3%)
- Number of SLICEs: 1706 out of 13696 (12%)
- Number of BUFGMUXs: 8 out of 16 (50%)
- Number of DCMs: 2 out of 8 (25%)
- Number of BSCANs: 1 out of 1 (100%)
- Number of ICAPs: 1 out of 1 (100%)

- Resource usage: PowerPC ≈ MicroBlaze
- Xilinx MicroBlaze soft processor ~950 logic cells (475 Slices)
# Resource Usage of IP Cores

<table>
<thead>
<tr>
<th>System Component</th>
<th>Resources Used</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Slices</td>
<td>LUTs</td>
<td>FFs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Min</td>
<td>Max</td>
<td>Min</td>
<td>Max</td>
<td>Min</td>
<td>Max</td>
<td></td>
</tr>
<tr>
<td>Required for Both Systems</td>
<td>46</td>
<td>436</td>
<td>81</td>
<td>668</td>
<td>5</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>OPB (On-Chip Peripheral Bus)</td>
<td>120</td>
<td>128</td>
<td>213</td>
<td>224</td>
<td>152</td>
<td>155</td>
<td></td>
</tr>
<tr>
<td>OPB HWICAP</td>
<td>25</td>
<td>34</td>
<td>16</td>
<td>30</td>
<td>33</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>OPB BRAM Controller</td>
<td>332</td>
<td>563</td>
<td>353</td>
<td>637</td>
<td>314</td>
<td>444</td>
<td></td>
</tr>
<tr>
<td>OPB DDR SDRAM Controller</td>
<td>523</td>
<td>1161</td>
<td>590</td>
<td>1559</td>
<td>504</td>
<td>799</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>523</td>
<td>1161</td>
<td>590</td>
<td>1559</td>
<td>504</td>
<td>799</td>
<td></td>
</tr>
<tr>
<td>Required for PowerPC System</td>
<td>223</td>
<td>1645</td>
<td>270</td>
<td>2540</td>
<td>59</td>
<td>484</td>
<td></td>
</tr>
<tr>
<td>PLB (Processor Local Bus)</td>
<td>595</td>
<td>836</td>
<td>535</td>
<td>823</td>
<td>547</td>
<td>812</td>
<td></td>
</tr>
<tr>
<td>PLB to OPB Bridge</td>
<td>N/A</td>
<td>N/A</td>
<td>37</td>
<td>57</td>
<td>52</td>
<td>82</td>
<td></td>
</tr>
<tr>
<td>Processor System Reset Module</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>PowerPC (Wrapper)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>77</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>818</td>
<td>2481</td>
<td>842</td>
<td>3420</td>
<td>658</td>
<td>1455</td>
<td></td>
</tr>
<tr>
<td>Required for MicroBlaze System</td>
<td>N/A</td>
<td>N/A</td>
<td>0</td>
<td>353</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2 x LMB (Local Memory Bus)</td>
<td>N/A</td>
<td>N/A</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>359</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Additional Features</td>
<td>N/A</td>
<td>N/A</td>
<td>88</td>
<td>108</td>
<td>48</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>OPB UART Lite</td>
<td>N/A</td>
<td>N/A</td>
<td>63</td>
<td>63</td>
<td>111</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td>OPB Timebase WDT</td>
<td>67</td>
<td>188</td>
<td>45</td>
<td>292</td>
<td>79</td>
<td>204</td>
<td></td>
</tr>
<tr>
<td>Microprocessor Debug Module</td>
<td>67</td>
<td>188</td>
<td>196</td>
<td>463</td>
<td>238</td>
<td>372</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>67</td>
<td>188</td>
<td>196</td>
<td>463</td>
<td>238</td>
<td>372</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- It is necessary to improve the security of SRAM FPGAs against different attacks.

- We propose a solution for secure partial reconfiguration that takes advantage of embedded processor cores and dynamic partial reconfiguration. It provides:
  - Feasible implementation for both hard/soft processor cores
  - Flexibility by using any arbitrary encryption/authentication software core
  - Reasonable resource utilization especially for processor-based systems

- Analyzing the available methods of partial reconfiguration for Xilinx FPGAs show:
  - A simple methodology along with more support and automation from tools are needed to:
    - Increase the ease of use for designers
    - Decrease the development time
Future Improvements

- Security Improvements:
  - Storing the partial bitstream in internal memory
  - Storing the key in the battery-powered storage

- Use of synthesizable Intellectual Property (soft IP) cores which can be readily incorporated into an FPGA for faster decryption and authentication

- Use of an embedded OS
The work has been accepted as a full paper for the presentation at the IEEE 2005 International Conference on Field-Programmable Technology (FPT' 05) in Singapore
Comments?

Questions?

Thank you