Holistic Security Design for the ThumbPod Embedded System

Herwin Chan
Doris Chang
Yi Fan
Alireza Hodjat
David Hwang
Bo-Cheng Lai

Yusuke Matsuoka
Patrick Schaumont
Kris Tiri
Dzi Tran
Shenglin Yang

Prof. Ingrid Verbauwhede
Embedded Security (EmSec) Group

http://www.ivgroup.ee.ucla.edu
Outline

• Embedded Security: Research Challenges
• Driver application: ThumbPod
• Issues we address:
  – Protocol
  – Algorithm
  – Architecture
  – Micro-Architecture
  – Circuit
• Putting it all together…
• Conclusions
Research Challenges

• The world is going **embedded** and **wireless**!!
• Wireless embedded security is
  – extremely important…
  – …yet unsolved!!

EmSec Mission: How to implement robust security on constrained devices?
Solution: Security Pyramid

- Partition security into five abstraction levels
  - Each level is secure only if lower levels secure
- Our research: design security at **ALL LEVELS** and ensure secure **TRANSITIONS** between levels
Driver Application: ThumbPod

- Currently, most biometric systems perform processing on server side
- Secure keychain device performs all biometrics and cryptography locally
- Components:
  - Microcontroller and memory
  - Fingerprint sensor
  - Biometric and cryptographic accelerators
  - IR and USB
Protocol Level:

Biometric Authentication Protocol

- Problem: security is weak between user and credit card
- Solution: biometric authentication protocols using biometrics and cryptography
- Security-energy tradeoffs based on local or server signal processing
Algorithm Level:
Embedded Fingerprint Matching

• Problem: How to fit floating-point fingerprint algorithm on constrained embedded devices
Algorithm Level: Embedded Fingerprint Matching

- Floating point NIST algorithm
  - Fixed point code and memory optimizations
  - New matching algorithm
- 50% energy reduction with equal detection accuracy
  - False Accept Rate = 0.01%
  - False Reject Rate = 0.5%

Reduction of the energy consumption for minutiae detection
Architecture Level:
Embedded Software Design

- Problem: How do you design SW for a secure embedded system?
  - Secure code: Java with cryptographic libraries and security functionality
  - But constrained embedded devices running Java are slow: require secure SW and HW acceleration
Architecture Level:
Embedded Software Design

- Solution: GEZEL environment for design of co-processors and cycle-through accurate simulations
- Each platform corresponds to the addition of an abstraction level
- Three simulation platforms of the same system
Architecture Level:
AES Crypto-processor Design

- Advanced Encryption Standard (AES) based on Rijndael Algorithm
- Symmetric key cipher using Galois Field Arithmetic
- First published IC implementation!
- Co-processor design of Rijndael cores
### Architecture Level:

**AES Crypto-processor Design**

<table>
<thead>
<tr>
<th></th>
<th>Java cycles</th>
<th>C cycles</th>
<th>Co-processor cycles</th>
<th>Total Cycles</th>
<th>Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>AES 301,034</td>
<td>Interface 367</td>
<td>AES 44,063</td>
<td>301,034</td>
<td>6.8X</td>
</tr>
<tr>
<td></td>
<td>Interface 892</td>
<td></td>
<td>AES 11</td>
<td>903</td>
<td>333X</td>
</tr>
</tbody>
</table>

- **Interface overhead for co-processor consumes cycles but still 333X improvement**
- **Better improvement if separate data and control flow**
  - Currently, data flow and control flow are merged
  - Co-processors with direct memory access would reduce interface overhead
Circuit Level: Combating Power Analysis Attacks

- Differential Power Analysis (DPA) exploits power properties of CMOS transitions
  - 0→0 no power dissipation
  - 0→1 power dissipation

- Our sense amplifier based logic (SABL) charges constant capacitance
  - Minimizes transition power variations
Circuit Level:
Combating Power Analysis Attacks

→ Reduction of power variation by 116x!
Putting it together…FPGA

- Protocol
- Algorithm
- Architecture
- Micro-Architecture
- Circuit

Simultaneous
Identification
Confidentiality
Integrity

Cipher Design, Biometrics

Java
JCA
KVM

CPU
MEM
Crypto

Vcc
CLK
Putting it together…FPGA

- Xilinx Virtex-II FPGA
  - Embedded LEON 32-b Sparc processor
  - Memory-mapped co-processors
Putting it together…FPGA

- Working demo on an FPGA board (two ThumbPods shown) and PC connected over RS-232
- Demonstration at DAC 2003 and today!!
Putting it together...ASIC

- Protocol ✓
- Algorithm ✓
- Architecture ✓
- Micro-Architecture ✓
- Circuit ✓
Putting it together...ASIC

- Secure ASIC Design
- Unprotected
  - LEON processor
  - Memory and buses
- Protected by SABL
  - AES crypto-processor
  - Matching oracle for secure matching decisions
  - Secure storage
Conclusion

• EmSec researches on all levels of the embedded security pyramid
  – Example driver: ThumbPod
• Other projects:
  – GEZEL for multi/co-processor simulation
  – Optical CDMA cryptography
  – Wireless sensor network security
Thank You