FPGAs for Trusted Cloud Computing

Ken Eguro
Embedded and Reconfigurable Computing

Ramarathnam Venkatesan
Cryptography, Security and Applied Mathematics

FPL 2012 – Oslo, Norway
August 29th
Cloud Computing

Traditional Servers

Datacenter

Client Control

Client

Cloud Servers

Datacenter

Cloud Manager

Client Control

Client
Cloud Security Issues

- Existing cloud systems cannot offer strong security guarantees
  - Cloud administrator access ➔ liability
  - Availability & co-tenancy ➔ malware & side-channel attacks

Cloud administrators have full access!
Cloud Security Issues

- Existing cloud systems cannot offer strong security guarantees
  - Cloud administrator access → liability
  - Availability & co-tenancy → malware & side-channel attacks

Cloud is open to everyone!
Service-Level Agreements

- Network bandwidth/latency
- CPU time
- Storage allotment/latency
- Minimum uptime
- Security
Observation: Security Imbalance

- 1% to 10% of information/transactions deal with sensitive data
- Isolate only sensitive computations on trusted compute nodes
Independent administration
  - Management != full access
  - Cloud operator is not part of “root of trust”

- Physically secure
- High performance
- Generality
- Flexibility
Trusted Compute Node

- Independent administration
- Physically secure
  - Store keys
  - Decrypt & authenticate binaries and data
  - Execute application exactly as prescribed
- High performance
- Generality
- Flexibility
Trusted Compute Node

- Independent administration
- Physically secure
- High performance
- Generality
- Flexibility
Process of Elimination

- **Requirements**
  - Independent administration ✓
  - Physically secure ✗
  - High performance ✓ ✓
  - Generality ✓
  - Flexibility ✓

- **Platform Options**
  - Commodity servers
  - Local/cloud hybrids
  - High security commodity servers
  - Secure co-processors
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs
Requirements
- Independent administration ✓
- Physically secure ✓
- High performance ✗
- Generality ✗
- Flexibility ✗

Platform Options
- Commodity servers
- Local/cloud hybrids
- High security commodity servers
- Secure co-processors
- Homomorphic crypto
- Dedicated hardware
  - HSMs
  - FPGAs
Process of Elimination

- **Requirements**
  - Independent administration ✓
  - Physically secure ✓
  - High performance ✗
  - Generality ✗
  - Flexibility ✓

- **Platform Options**
  - Commodity servers
  - Local/cloud hybrids
  - High-security commodity servers
  - Secure co-processors
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs
Process of Elimination

Requirements
- Independent administration ✓
- Physically secure ✓
- High performance ✓
- Generality X
- Flexibility X

Platform Options
- Commodity servers
- Local/cloud hybrids
- High security commodity servers
- Secure co-processors
- Homomorphic crypto
- Dedicated hardware
  - HSMs
  - FPGAs
Process of Elimination

- **Requirements**
  - Independent administration ✓
  - Physically secure ✓
  - High performance ✓
  - Generality ✓
  - Flexibility ✓

- **Platform Options**
  - Commodity servers
  - Local/cloud hybrids
  - High security commodity servers
  - Secure co-processors
  - Homomorphic crypto
  - Dedicated hardware
    - HSMs
    - FPGAs
Infrastructure Setup

FPGA Platform Board

Dedicated Resources

FPGA
- Onboard Key Mem.
- Onboard Boot. Logic

Programmable Logic Region
Infrastructure Setup

FPGA Platform Board

- FPGA
- Onboard Key Mem.
- Onboard Boot. Logic

Trusted Authority

- Bitstream Key
Loading Application Binaries

- **Untrusted Cloud Machine**
  - **FPGA Platform Board**
    - **FPGA**
      - **Onboard Key Mem.**
      - **Onboard Boot. Logic**
  - **Untrusted Cloud Machine**

- **FPGA Platform Board**
  - **Platform Memory**
    - **Bitstream Key**
      - **Customer Application**
      - **Customer**

- **Trusted Authority**
Loading Application Binaries

Untrusted Cloud Machine

FPGA Platform Board

FPGA

Onboard Key Mem.

Encrypted & Signed Bitstream

Onboard Boot. Logic
Dynamic Deployment

Client Application

Application Request

Untrusted Cloud Machine

FPGA Platform Board

FPGA

Onboard Key Mem.

Encrypted & Signed Bitstream

Onboard Boot. Logic

Loaded Application

Client
Advanced Issues – TA Interaction

Trusted Authority

Bitstream Key

Remove per FPGA bitstream?

Platform Memory

Untrusted Cloud Machine

FPGA Platform Board

FPGA

Onboard Key Mem.

Onboard Boot. Logic

Remove TA involvement?

Customer Application

Customer
Medical record tokenization

- Sensitive vs. non-sensitive data
Medical record tokenization

- Sensitive vs. non-sensitive data
- Separate, tokenize & encrypt sensitive fields

Client App → Data Stream → Trusted Computing Node

- Identify sensitive fields
- Non-Sensitive Plaintext → Anonymization
- Tokenized Data

Bulk Cloud Servers

Data Mining

Results
Medical record tokenization

- Prototype cloud server & FPGA architecture
## Resource Requirements

- **On an ML605 (V6 LX 240T)**

<table>
<thead>
<tr>
<th></th>
<th>LUTs</th>
<th>FF</th>
<th>BRAM</th>
<th>DSP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Full system</strong></td>
<td>18.1%</td>
<td>9%</td>
<td>6.9%</td>
<td>0.5%</td>
</tr>
</tbody>
</table>
| **Infrastructure**
  (RSA, SHA, PCIe, DDR3) | 14.8%  | 8.6%  | 5.2%  | 0.5% |
| **Tokenization**
  (AES, AES + SHA) | 3.3%   | 0.3%  | 0.7%  | 0.0% |
Performance

- On an ML605 (V6 LX 240T)
  - 200MHz clock
  - Initiate 13+ RSA secure session key exchanges per second
    - Decrypt AES at 572MB/s
    - Tokenize with SHA-256 at 12MB/s
- Gb Ethernet is 125MB/s
- 1-10% of the incoming data was sensitive
Conclusions

- Security is paramount to the cloud
- Existing servers are insufficient
- FPGAs provide native support for secure boot and secure operation
- This represents a brand new market for FPGAs