Hardware Support for High-Performance, Intrusion- and Fault- Tolerant Systems

Giacinto Paolo Saggese, Claudio Basile, Zbigniew Kalbarczyk, Ravishankar K. Iyer

MOTIVATION
- Providing high performance to secure and reliable systems is challenging
- Most intrusion-tolerant solutions are software only
- Critical applications need high performance:
  "eBay lost $5M in fees and 20% of their market capitalization whilst traffic to their competitor sites increased by 50% as a result of the inability to satisfy user demand" , Nov 2000

ARCHITECTURE
- Parallel FPGA Crypto-Engine
- Active replication with Multithreaded Replicas
- Threshold Cryptography

CRYPTO-ENGINE ARCHITECTURE
FPGA-based PCI card containing:
- 15 instances of RSA Processors
- Tamper-resilient Key-Store
- Main Controller

SECURITY ANALYSIS
Goal of attacker is to forge Attribute Authority signature
Threshold cryptography guarantees that this cannot happen unless a majority of replicas are compromised
Attacker can achieve his goal by:
  - Stealing secret keys from a majority of replicas, or
  - Taking control of a majority of replicas
This can be done at:
  - Hardware level - physical attack to Crypto-Engine device
  - Software level - remote attack

OPERATION
Fanout-Combiner
- Forwards certificate requests certReq to replicas
- Collects replica outputs (certi, Xi, Pi)
- Performs majority voting on certi
- Assembles partial signatures Pi to produce certificate signature Y
- Verifies Y to identify and exclude compromised replicas

Certificate Engine Replicas
- Multiple threads serve client requests concurrently by using attached Crypto-Engine to compute partial signatures Pi
- PDS algorithm schedules threads' mutex requests deterministically (to enforce replica consistency)

EXPERIMENTAL EVALUATION
Three main-configurations:
- Baseline - no replication, no threshold cryptography
- Triplicated with no threshold crypto - each replica has common service key D
- Triplicated with threshold crypto - each replica has a different share Si of service key D
Each configuration comes in two flavors:
- Software - crypto operations done in software
- Hardware - crypto operation done with hardware Crypto-engine
The triplicated configuration (with voting) use:
- PDS algorithm, or
- NPDS algorithm

METRICS
- Throughput is the number of certificates for second
- Overhead with respect to no replication and no threshold cryptography
- Speedup with respect to software configuration

<table>
<thead>
<tr>
<th>Certificate Engine Configuration</th>
<th>Throughput [ACs/sec]</th>
<th>Overhead</th>
<th>Speedup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline</td>
<td>5.71</td>
<td>N/A</td>
<td>8.1</td>
</tr>
<tr>
<td>Triplication without Threshold Crypt. (PDS)</td>
<td>5.71</td>
<td>44.9</td>
<td>2.7%</td>
</tr>
<tr>
<td>Triplication without Threshold Crypt. (NPDS)</td>
<td>5.70</td>
<td>3.36</td>
<td>1200%</td>
</tr>
<tr>
<td>Triplication with Threshold Crypt. (PDS)</td>
<td>5.60</td>
<td>44.5</td>
<td>3.6%</td>
</tr>
<tr>
<td>Triplication with Threshold Crypt. (NPDS)</td>
<td>5.32</td>
<td>3.35</td>
<td>1200%</td>
</tr>
</tbody>
</table>

www.iti.uiuc.edu
University of Illinois at Urbana-Champaign