Trlnc: Small trusted hardware for large distributed systems

D. Levin, J. Douceur, J. Lorch and T. Moscibroda
Presented by Clint Sbisa

March 8, 2010
Introduction

- TrInc: Trusted incrementer
- Monotonic counter and a key
- Trusted Platform Module (TPM)
Background

- Equivocation
- Trusted hardware
Design

- Preventing equivocation
- API depends on internal state
- Trinkets (communicate over USB or other channel)
Design

- Private/public key and identity
- Attestations
- Certificates
- Checking attestations
- Counters (and metacounter)
- Queue of attestations
Analysis

- Equivocation
- Timeliness
- Minimality
Case study: A2M

- Trusted logs (append)
- Attestations for actions (appending, deleting, lookups)
- Decreased complexity
Enabling accountability by using witnesses
Interaction among witnesses
Clear proof of misbehavior
Challenge-response no longer needed, no witness-to-witness communication
Case study: BitTorrent

- Open incentives
- Under-reporting pieces to peers to obtain higher download
- Count number of pieces received
## Implementation

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noop</td>
<td>6.14 ± 0.15</td>
</tr>
<tr>
<td>Attest (asymmetric, advance &gt; 0)</td>
<td>230.24 ± 0.28</td>
</tr>
<tr>
<td>Attest (asymmetric, advance = 0)</td>
<td>198.21 ± 0.10</td>
</tr>
<tr>
<td>Attest (symmetric, advance &gt; 0)</td>
<td>128.95 ± 0.08</td>
</tr>
<tr>
<td>Attest (symmetric, advance = 0)</td>
<td>105.90 ± 0.08</td>
</tr>
<tr>
<td>Verify Symmetric Attestation</td>
<td>85.81 ± 0.11</td>
</tr>
</tbody>
</table>

- Gemalto .NET SmartCards
- Slow!
## Evaluation: A2M

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (msec)</th>
<th>TrInc</th>
<th>A2M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Noop</td>
<td></td>
<td>6.99 ± 0.01</td>
<td></td>
</tr>
<tr>
<td>Append</td>
<td>187.60 ± 0.15</td>
<td>551.93 ± 154</td>
<td></td>
</tr>
<tr>
<td>Lookup (Successful)</td>
<td>0.0122 ± 0.02</td>
<td>304.14 ± 6.87</td>
<td></td>
</tr>
<tr>
<td>Lookup (TooEarly)</td>
<td>162.24 ± 0.08</td>
<td>289.68 ± 2.23</td>
<td></td>
</tr>
<tr>
<td>Lookup (Forgotten)</td>
<td>162.35 ± 0.10</td>
<td>350.51 ± 1.43</td>
<td></td>
</tr>
<tr>
<td>End</td>
<td>162.31 ± 0.11</td>
<td>294.16 ± 2.04</td>
<td></td>
</tr>
<tr>
<td>Truncate</td>
<td>187.94 ± 0.10</td>
<td>28.99 ± 0.02</td>
<td></td>
</tr>
<tr>
<td>Advance</td>
<td>187.81 ± 0.12</td>
<td>288.20 ± 11.4</td>
<td></td>
</tr>
</tbody>
</table>
Evaluation: PeerReview

The bar chart shows the average traffic (Kbps per node) for different numbers of witnesses.

- **Baseline**
- **1**
- **2**
- **3**
- **4**
- **5**

The chart compares two categories:
- PeerReview
- TlInc

The traffic increases as the number of witnesses increases, with PeerReview generally showing higher traffic than TlInc.
Evaluation: BitTorrent
Conclusion

- Need for hardware
- Slow— not acceptable for some protocols
- Adoption