Reducing the Trusted Computing Base

David Lie
Department of Electrical and Computer Engineering
University of Toronto
TCB’s are Complex

- Trusted Computing Base: The components of a system that an application must trust to function correctly

![Diagram showing TCB components: Application (Application Dependent), Application Libraries (10K’s of LOC), Other Applications (Millions of LOC), Operating System & Hardware (Millions of LOC)]

- Total Exposure for an application is in the millions to 10’s of millions of LOC at least!
One approach is to isolate the application in a separate VMM [Terra]
- VMM is added to the TCB, but TCB is still reduced because unrelated applications are removed

<table>
<thead>
<tr>
<th>Application (Application Dependent)</th>
<th>Application Libraries (10K’s of LOC)</th>
<th>Other Applications (Millions of LOC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System (Millions of LOC)</td>
<td>Operating System (Millions of LOC)</td>
<td></td>
</tr>
<tr>
<td>Virtual Machine Monitor (10K’s LOC)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reducing the TCB

• However, the isolated application still has a TCB of millions of LOC:
  – Can we do better?
Total TCB Reduction

• Millions of LOC → 10K’s LOC ~ 100x reduction
  – OS is customizable for each component, only has functionality the component needs

• Small TCB can be made more secure:
  – Easier for code audit
  – Many tools (static and dynamic) scale exponentially with the size of code
  – Less effort/cost to harden smaller code base
  – Can be protected by implementing in safer language