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

Application
(Application Dependent)

Application Libraries (10K's of LOC)

Other Applications (Millions of LOC)

Operating System & Hardware (Millions of LOC)



Isolate Application in a Separate VMM

- 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



Application Libraries (10K's of LOC)

Other Applications (Millions of LOC)

Operating System (Millions of LOC)

Operating System (Millions of LOC)

Virtual Machine Monitor (10K's LOC)



Reducing the TCB

 However, the isolated application still has a TCB of millions of LOC:

Can we do better? Application Other Applications Libraries (Millions of LOC) (10K's of LOC) Security Critical Component Minimal OS **Operating System** (~10K LOC) (Millions of LOC) Virtual Machine Monitor (10K's LOC)

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

