Minimizing the Trusted Computing Base

Mahalingam Ramkumar
Associate Professor
Department of Computer Science and Engineering

Mississippi State University
What and whom exactly we trust when we say that

- This roof will not fall on our heads · · ·
- This car will not burst into flames · · ·
- This nuclear plant will function as it should · · ·
- Our network infrastructure is reliable · · ·
Trusted Computing Base

The minimal amount of hardware/software that needs to be trusted to justify our assumption

- Our research envisions this to be a trusted chip
- Simple, verifiable, and fixed functionality
- No other hardware/software trusted
What is the fixed functionality required for

**Application Domains**
- A Domain name system server?
- A SCADA system?
- A mobile ad hoc network?
- BGP routers in our network infrastructure?

**Building Blocks**
- Efficient cryptographic mechanisms for authentication of severely resource limited modules
- Ordered Merkle tree - a mechanism for a resource limited entity to maintain the integrity of a dynamic data base of any size.