

HCSS: NEC4CPS
Pittsburgh 11/08-09, 2006

**Real-Time Isolation and Composition
of Virtualized Resource Sets**

Aloysius K. Mok
University of Texas at Austin

Important Technical Challenges

- Where is the weakest link from attacker's point of view?

Reliable, secure distributed control over wide-area networks depends on

- Complete mediation (authentication, integrity, authority)
- Predictable QoS (latency, bandwidth, power)
- Cooperation of administrative domains
- Survivability under deliberate attack
 - Determination of damage
 - Containment and reconfiguration

Most Important Information Technology Research Needs

Concede defeat. Need to mitigate damage by containment (what have we lost?) and recovery by self-healing, attack-resistant execution platforms

- Define resource configuration space for distributed control
 - Virtualization is the key
- Virtualization must take into account QoS, fault tolerance and security properties
 - What resource set is required to implement what distributed control strategy?
 - What resource set can be composed?

Possible Roadmap for the Next 5-10 Years

- Revisit virtualization in a fundamental way
 - What is the appropriate abstraction?
- Investigate composition methods for constructing virtual resource sets from physical resource sets
 - Processors + I/O
 - Routers, network overlays
 - Sensors
- Testbed and incremental deployment