

# **Distributed Trust: Support Fault-tolerance and Attack- tolerance**

Fred B. Schneider and Lidong Zhou

presented by Chi Bun Chan

Nov 1, 2004

# Distributed Trust

- A paradigm yielded from the coupling of replication with threshold cryptography for use in environments satisfying weak assumptions.
- Trustworthy Services
  - Implementing fault-tolerance (benign) and attack-tolerance (malicious)
  - Basic recipe and existing designs are inadequate

# Revisiting Fault-tolerant Replications (1)

- Deterministic State Machine Replication Systems
  - Flexible service semantics under deterministic state transitions
  - Client requests trigger state transitions
  - Replica-coordination to agree on orders of client requests

