

# Dynamic Trust Management (DTM)

Jonathan M. Smith (Co-PI)  
Computer and Information Science  
University of Pennsylvania

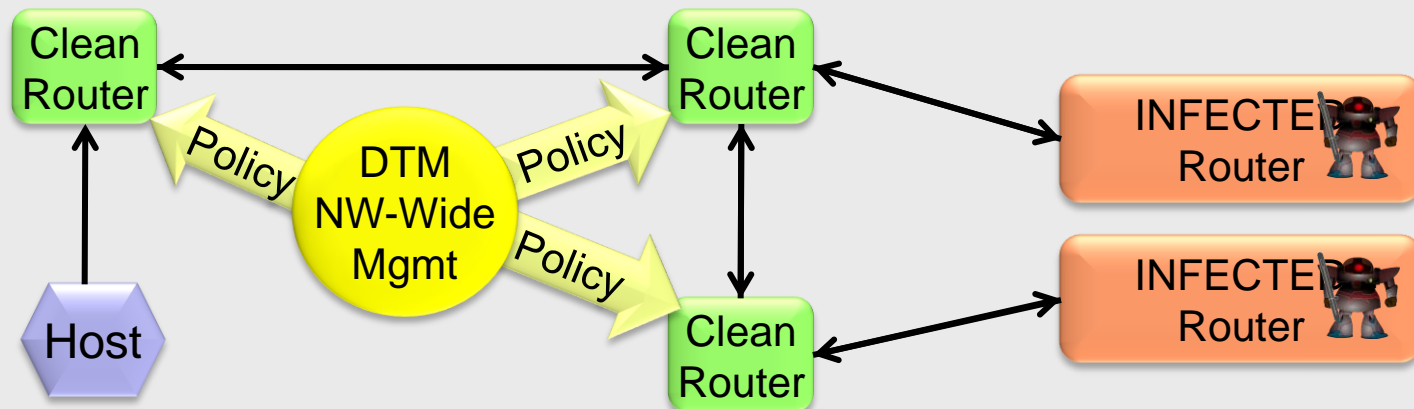
ONR MURI N00014-07-1-0907

Review Meeting

November 4, 2009

# Dynamic Trust Management

- A **COOPERATIVE** and **DYNAMIC** policy evaluation infrastructure enables such critical capabilities as:
  - Adaptation to dynamic service availability
  - Complex situational dynamics (e.g., differentiating between botnet and physical attacks on infrastructure).
- **BENEFITS** of a Dynamic Trust Management (DTM) approach
  - Flexible and robust control of authorizations in complex distributed systems such as the DoD/IC GIG, Navy FORCEnet and Clouds
  - The ability to define policies for scalable decentralized defense against emergent cyber-threats by rapid adaptation of resource access limits.

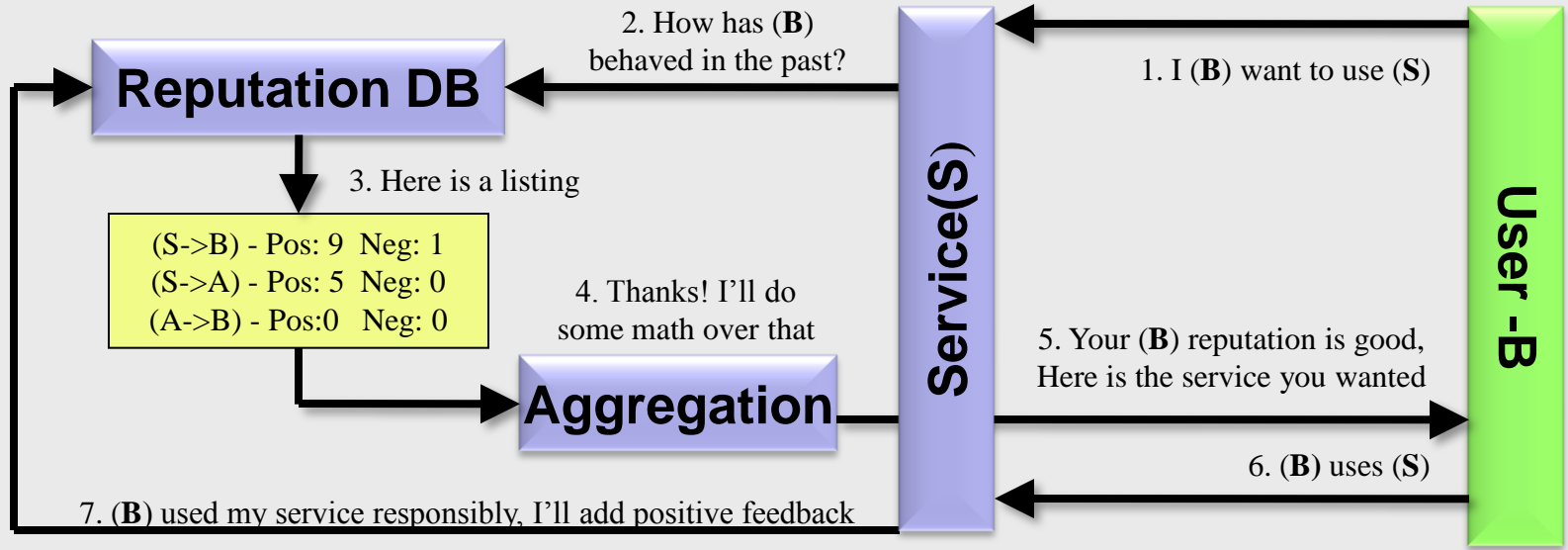


# MURI Challenges for DTM to address

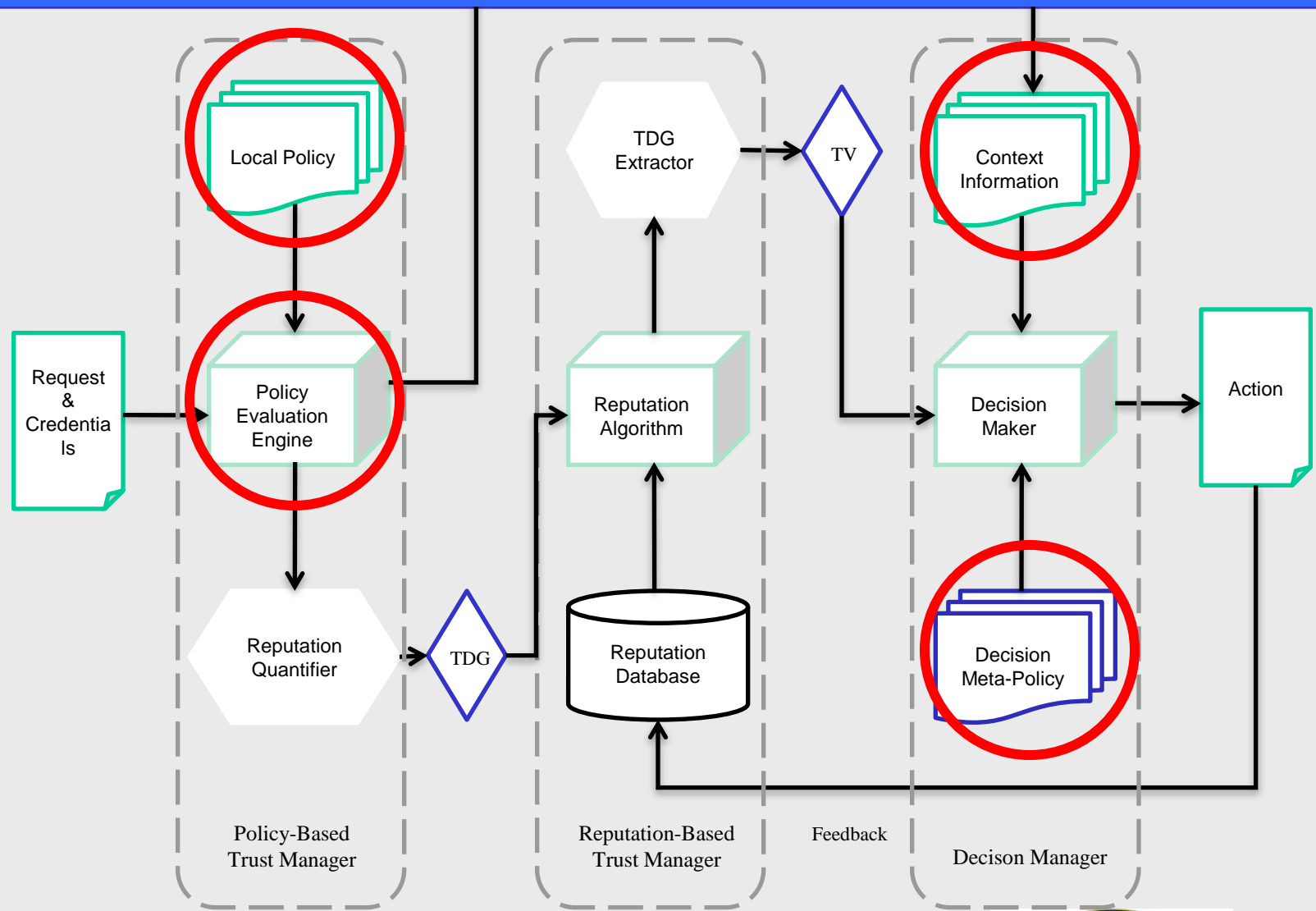
- TM policies are static; centralized compliance chk
  - Situations are dynamic (policies + principals)
  - Situations are distributed
- What is needed?
  - *Dynamic policies* to reflect situation dynamics
  - *Reputations* for principal dynamics
  - *Cooperative architecture* suited to GIG, Navy FORCEnet and emerging Cloud Computing
- Can we make it usable and perform well?

# Reputation-Based TM (RTM)

- Trust valuation based upon prior interaction history between two parties
  - Discovers new trust relationships based on partial, uncertain information
  - Accounts for indirect interactions
  - Combines multiple trust chains
  - Captures a degree in  $[0,1]$  that A trusts B
  - Uses feedback to dynamically adjust reputation values

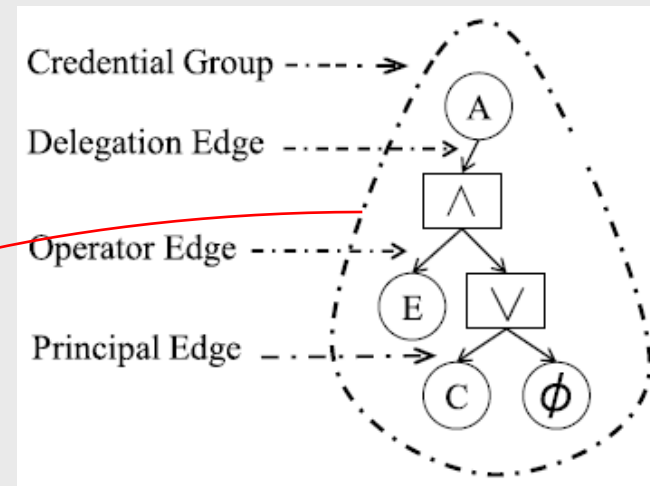
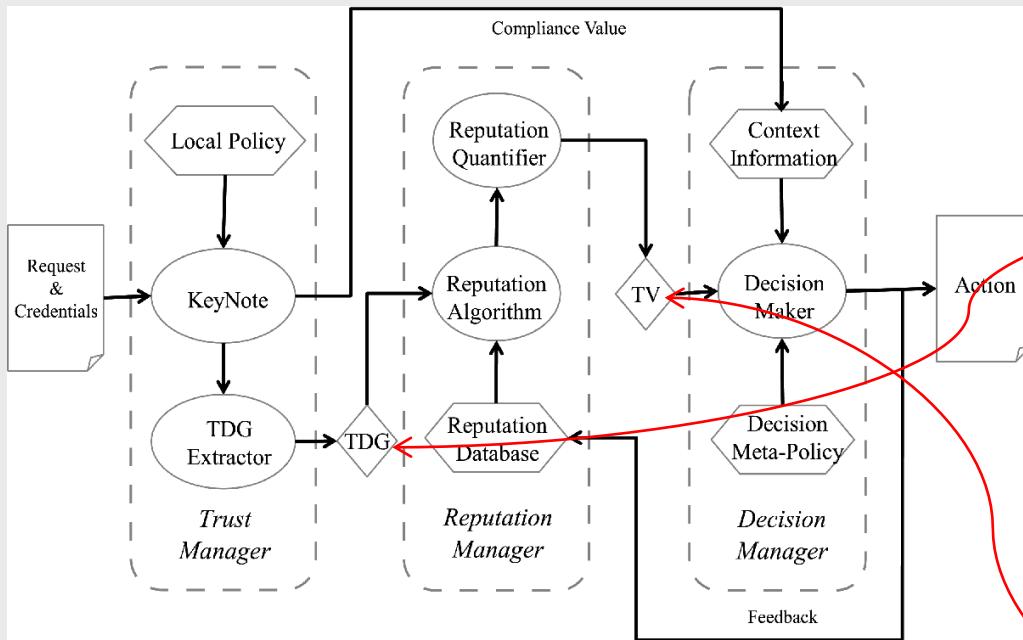


# DTM enables and exploits QTM



# A QTM instantiation: QuanTM

- QTM provides a *dynamic* interpretation of authorization policies for access control decisions using evolving reputations of parties
- *QuanTM* is a QTM system that combines elements from PTM and RTM to create a novel method for trust evaluation



Trust Dependency Graph (TDG), encoding PTM relationships useful for RTM

Reputations of PRINCIPALS, DELEGATIONS and CREDENTIALS are aggregated

## The QuanTM Architecture

# QuanTM Implementation Status

Module Based, plug and play

## – KeyNote as Policy Language

- New Python Implementation ~4000 lines
  - <http://experience2.org/wiki/index.php?n=EzPyKeynote.EzPyKeynote>
- Outputs CV and TDG in XML format

## – Mysql as Reputation Database

## – TNA-SL as Reputation Logic

- New Java Implementation ~4000 lines
- Inputs: TDG, Reputation DB; Output: Trust Value
  - <http://rtg.cis.upenn.edu/qtm/quantm.php3>



# Performance: *policy stability*

- Location tracking of smartphone users shows:
  - Repeated travels – behavioral patterns
- Therefore, even with DTM, *limited policy churn!*
  - Small set of policies may be enough

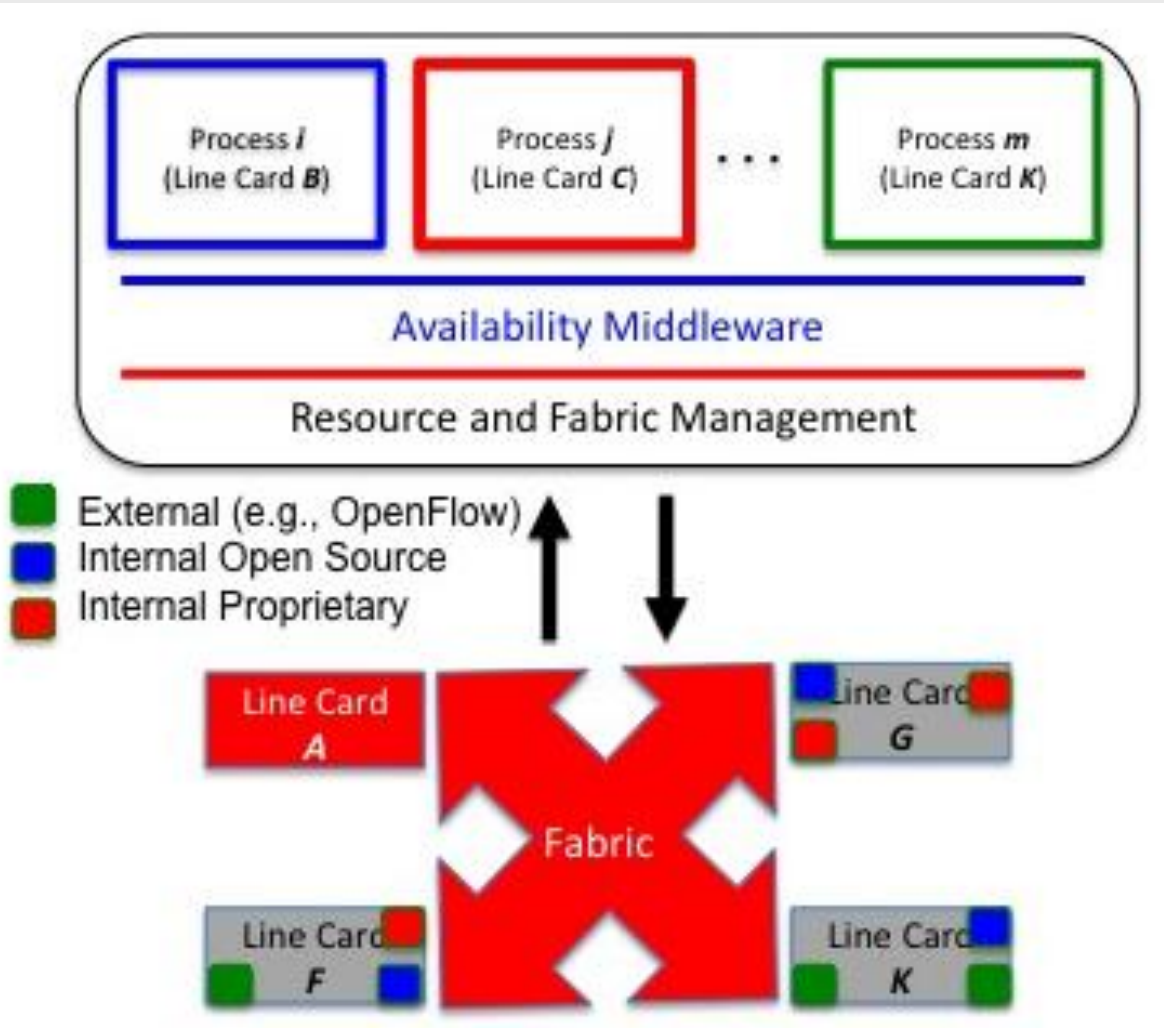




# DTM Impact

- Influence on router architecture through R3 (next)
  - Working on module distribution
- Influence on malware defense policies
  - Working on detection/mitigation w/ISP #1
- Influence on botnet defense policy deployment
  - Working on cooperative detect/mitigate, ISP #2
- Influence on DARPA Intrinsically-Assurable Mobile Ad-Hoc Network (IAMANET) Zodiac project

# DTM Outreach: R3\* Architecture



\* R3 is Router Reliability Research and is described in a white paper available at

<http://r3.cis.upenn.edu>

Penn, Cisco, Cornell, Delaware, MIT, Purdue and Vrije Universiteit are currently involved

# Work in MURI Continuation

- QuanTM-managed Wiki as test application
  - Test of QTM's fused policies and reputations
- Demonstrate use in novel botnet defenses
  - Use QuanTM to check data access
  - Use QuanTM to check policy downloads
- Real-world data to examine issues at scale
  - Dynamics from internal and ISP traces
- Tech transfer to router vendors and ISPs