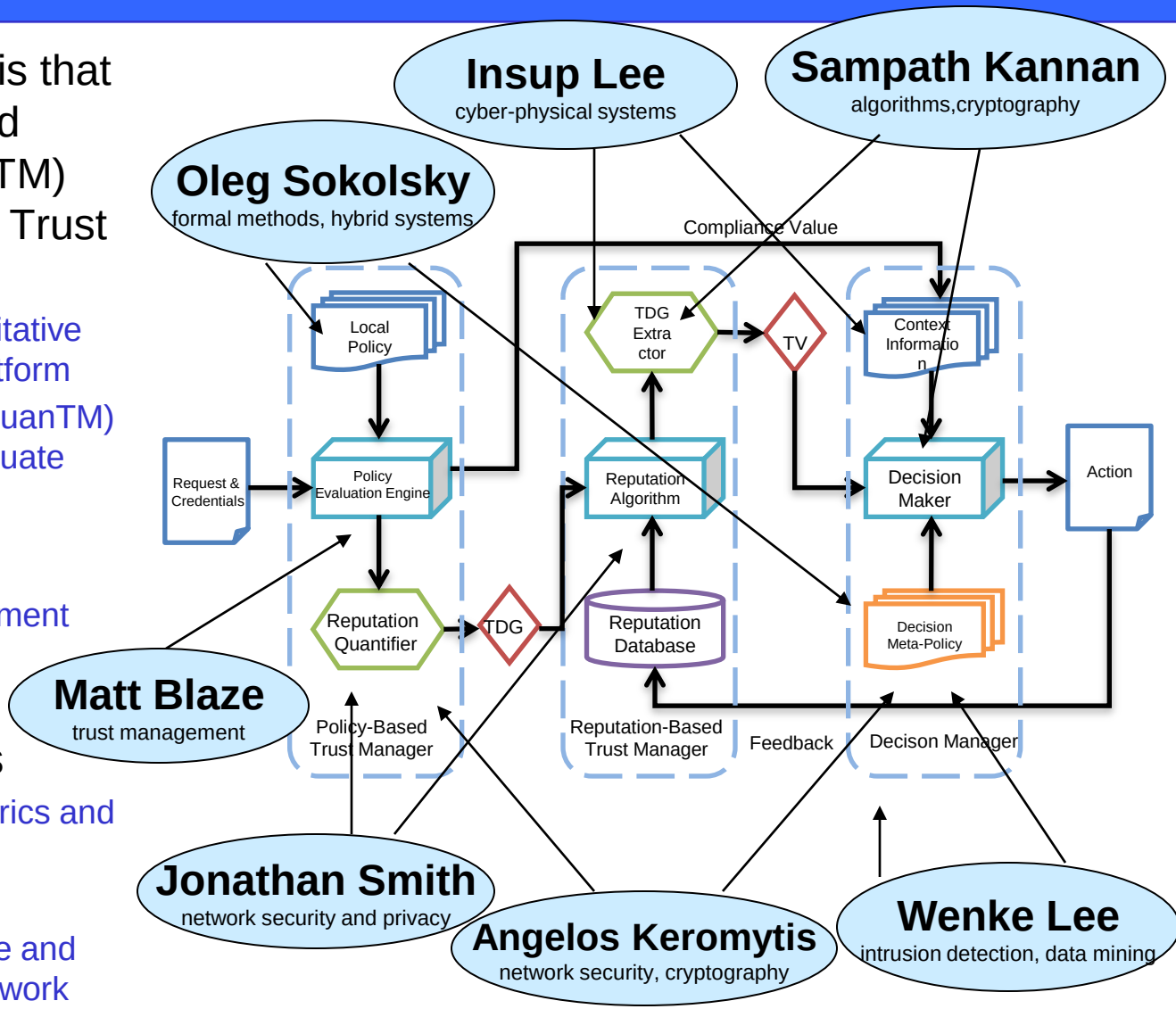
Conclusion and Future Work

Insup Lee
Computer and Information Science
University of Pennsylvania

ONR MURI N00014-07-1-0907
Review Meeting
June 10, 2010

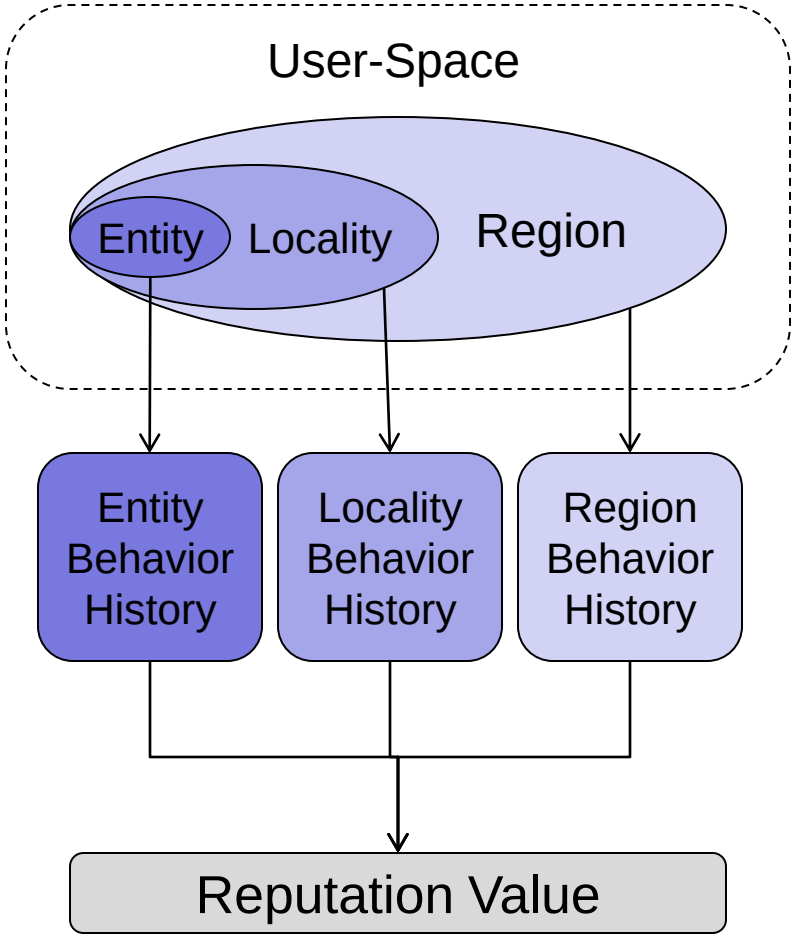
Summary

- Develop semantic basis that integrates Policy-based Trust Management (PTM) and Reputation-based Trust Management (RTM)
  - Develop a QTM (Quantitative Trust Management) platform
  - Implement prototype (QuanTM) and experimentally evaluate
- Extend PTM systems
  - Permission to speak
  - Dynamic Trust Management
  - Coordinated Policy Enforcement
- Improve RTM systems
  - Develop evaluation metrics and extensible simulator
  - Identify attack models
  - Design a highly effective and resilient RTM/FM framework



RTM: Spatio-Temporal Reputation

- Generalize and Formalize
  - Insight for general model?
  - Picking spatial groupings
    - Distance functions in non-IP-space situations?
  - Output values
    - Probabilistic characterization
    - Normalization considerations
- Case studies
  - Wikipedia
  - Facebook
- Connection to homophily in social networks



Reputations under delayed under uncertain feedback

- A receives a combined service from service providers X, Y, and Z
- A learns whether this service was “good” only over time
- If the service is faulty, A knows the probability that the fault is due to each of X,Y, and Z
- Under these conditions, how should reputations be computed? How should reputation managers aggregate reputations?

RTM: Reputations and Games

- Model adversaries as economic agents
- Define and analyze reputations using game-theoretic machinery
- Build mechanisms and incentives that will encourage agents to behave properly while maximizing social welfare
- Codify optimal (self-interested) behavior as policy and integrate with policy-based trust management
- Reconcile economics view with real systems - where do we get payoffs, strategy lists from?

Distributed TM

- Integrate with QTM
  - Particularly important in federated environments (e.g., dynamically composable SOAs)
- Efficiency of implementation; systems issues
- Large-scale case study
- Investigate the use of reactive mechanisms
  - Global coordination of dynamic defenses
- Investigate the use of active deception
  - Possible integration in NCR (National Cyber Range)

QTM for SIE (Security Information Exchange)

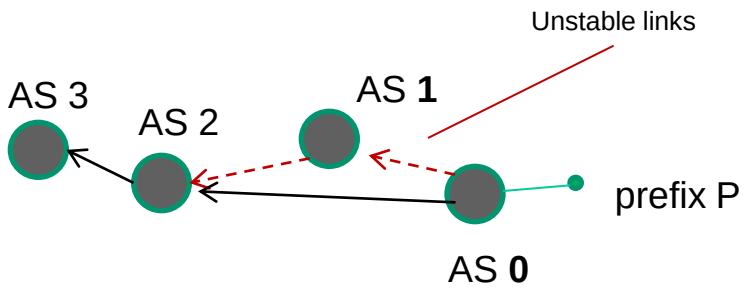
- Goal: develop dynamic trust management systems for Internet principals and services
  - E.g., IP addresses, DNS domains/servers, BGP/AS, etc.
  - Avoid connections to/from malicious/fraudulent elements on the Internet
- Progress thus far
  - Build an infrastructure, SIE, for collecting real-time Internet security information (GT)
    - Operational; data sources for dynamic trust management
  - SIE data used for studies of
    - Dynamic IP reputation using DNS data (GT)
    - Spatial-temporal reputation of IP from spam and WIKIPEDIA data (Penn)
  - Economics and games (Penn)
- Future work
  - Integrate IP reputation work at GT and Penn, in particular, GT can use the more formal and rigorous reputation models developed by Penn
  - Incorporate ideas of economics and games in reputation scoring to incentivize good behaviors

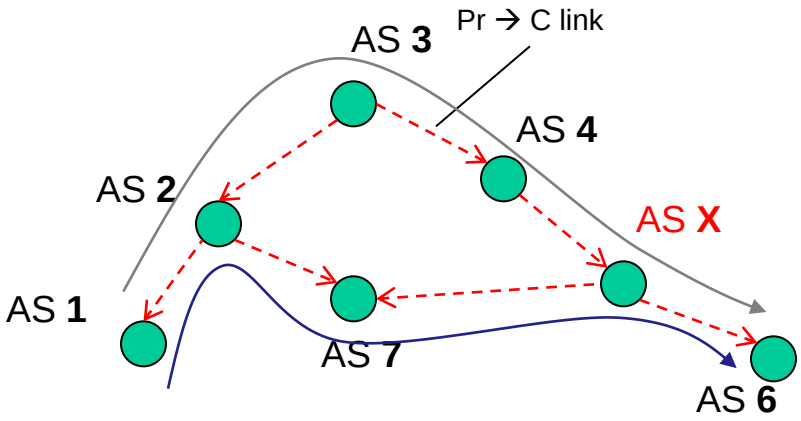
QTM-BGP: Improvements

- New behaviors of interest
  - *AS-link Stability*
    - How long do specific AS-links last
    - Path with unstable links should not be chosen
    - AS which announce such path penalized
  - *Policy Violation*
    - An AS violates valley-free and route preference policies. For example:
    - Valid path:
      - AS1→ AS2 → AS3 → AS4 → ASX → AS6
    - Violation:
      - AS1→ AS2 → AS7 → AS X → AS 6
      - AS 7 has two providers AS 2 and AS X

- Improved Reputation Model
  - Probabilistic interpretation of reputation, e.g., based on Bayesian statistics
  - Consider Good feedback in reputation

AS Link Stability

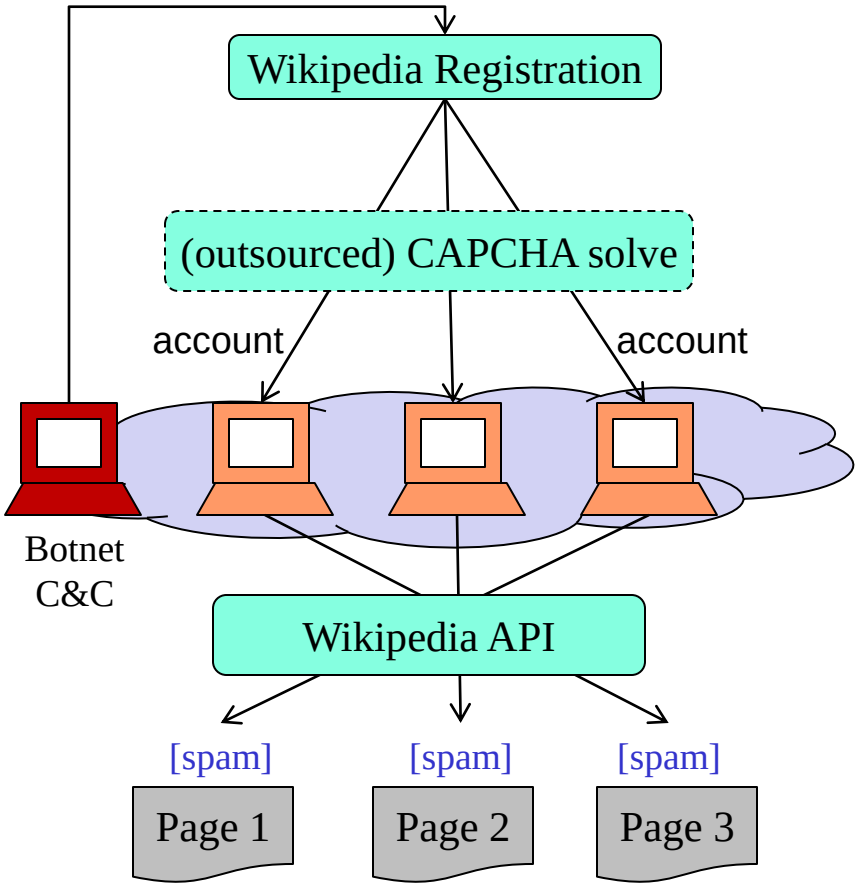




Valley Free Routing

Wiki Spam and Reputation Evasion

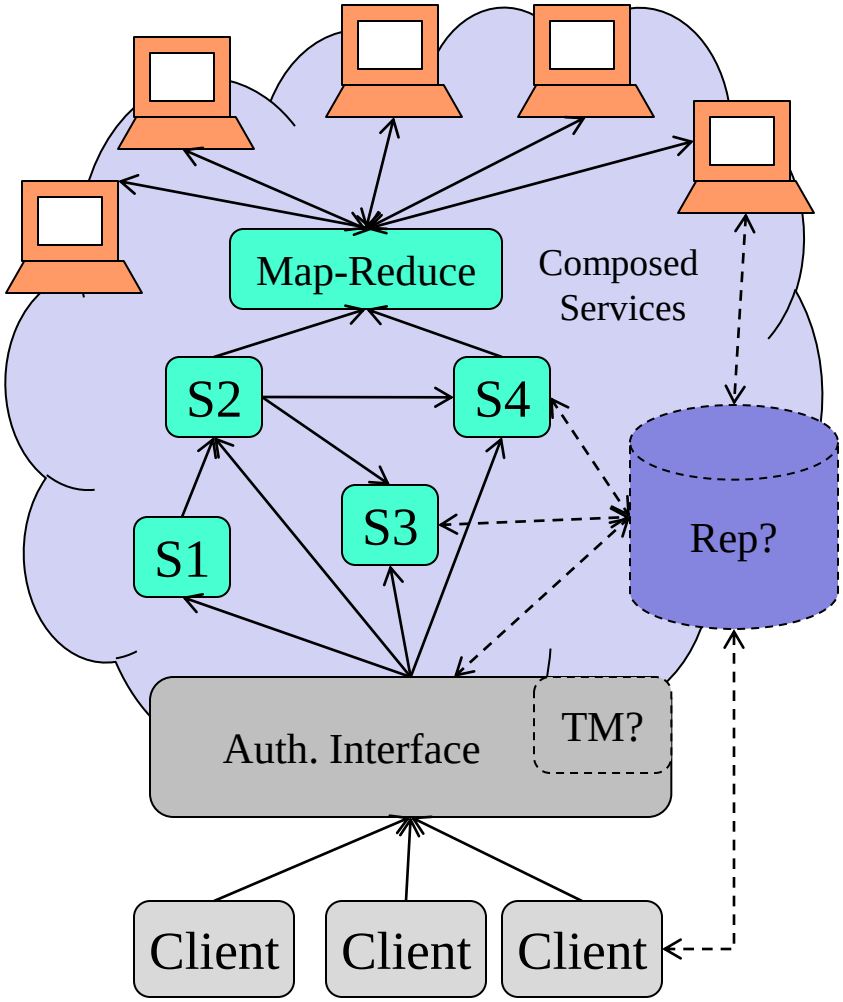
- Most Wikipedia *vandalism* is immature, but *spam* could be added by incentivized editors
  - Thus, more sophistication in their attacks and attempts at evasion
  - Evasion tactics: (1) time-of-day, (2) article popularity, (3) redirection, (4) inaccurate descriptions… How well do they work?
  - Could wiki-spamming be more profitable than email spam? (one revision == many views)
  - A wiki-spam bot? (see right)
- Benefit to QTM
  - Understand evasion of reputation mechanisms from real data set
  - Development of protection models
  - Broader applicability: emails/blogs



Potential Spam-Bot Attack against Wikipedia

QTM in the Cloud

- Trust Between…
  - Client → Service
  - Client → Service Provider
  - Service → Service
  - Federated Services, *etc.*
- Cloud Challenges
  - Migration and virtualization means reputation must be very dynamic
  - How to combine & valuate hardware/ service/client-level metrics?
  - Maintaining security guarantees across diverse architecture
- Why QTM?
  - QTM for mashup
  - High level of feedback sharing and density = greater accuracy.
  - Persistent ID: 1 client, many services



Cloud Computing Service Quality

- Outage/misbehavior of Cloud might lead to serious consequences.
- Questions:
  - What if SLA (Service Level Agreement) has been violated?
  - How can end-user detect such violations?
  - How long it takes to detect such violations?

- Develop Trust Establishment Tool to have better understanding of the behavior model of Cloud.
  - PTM: Cloud administrators should be able to specify policy to prevent undesired information leakage by the tool.
  - RTM: Customers can use it to query for specific information about cloud on behaviors (potentially application-specific) of interest, and provide feedback to build reputation scores for different Cloud providers.

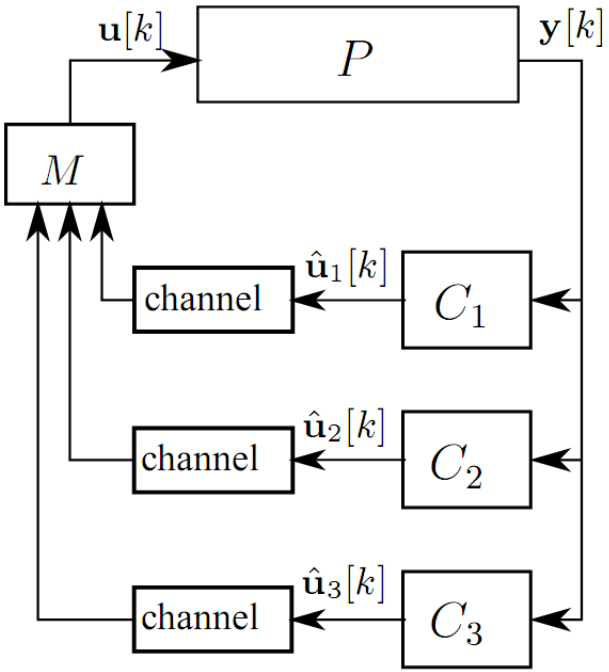
  - It should be easy to deploy on the cloud infrastructure.
  - It should scale to a large/real-world cloud.

QTM for CPS (Cyber Physical Systems)

- Integrate cyber and physical trusts
  - Interactions between cyber and physical systems
- Issues
  - Authentication/provenance of physical stimuli
  - Environmental uncertainty
- PTM for physical systems
- RTM for physical systems
- Case studies
  - Voting machines
  - Emergency management

QTM for Networked Control System

- Redundant networked controllers are useful as they provide the ability to tolerate faults and malicious behaviors in the controllers.



- However, given:
  - the lossy channel between the controllers and manager,
  - the probability of some of the controllers to be malicious or faulty

  it is possible that the outputs received from them are incorrect (application of which will affect the stability of the plant).

- We plan to incorporate this notion of trust in Network Controllers by integrating a Reputation Management System for them to improve the decision making process.


Penn
Engineering


DEPARTMENT OF THE NAVY
USN
ONR
Science & Technology

THANK YOU!