Conclusion and Future Work

Insup Lee

Computer and Information Science

University of Pennsylvania

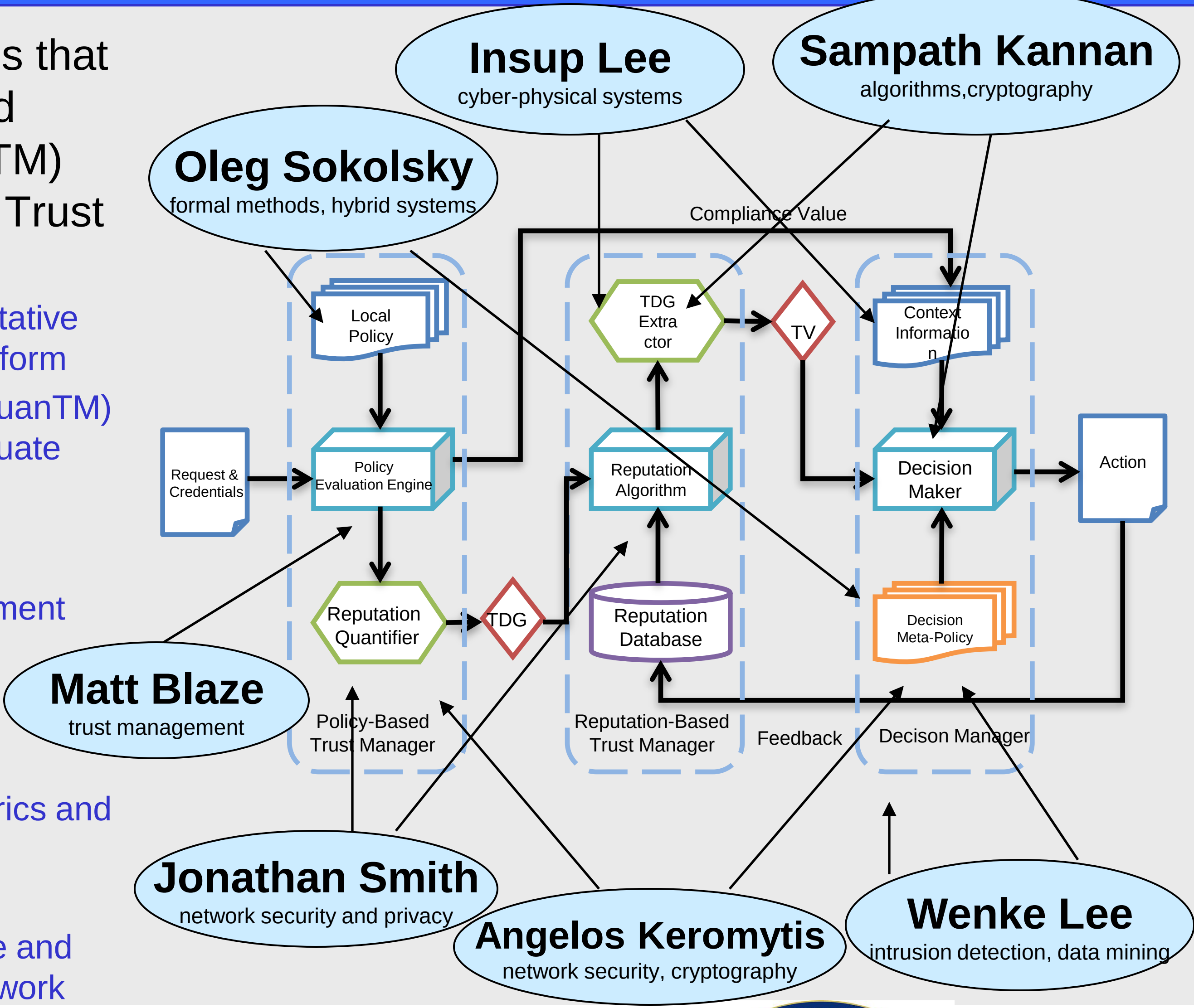
ONR MURI N00014-07-1-0907

Review Meeting

November 4, 2009

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



Proposed work

- PTM: Extensions to PTM
- RTM: Extensions to RTM
- QTM: Integration into QTM
- Distributed TM
- QTM Applications

PTM: Extensions to PTM

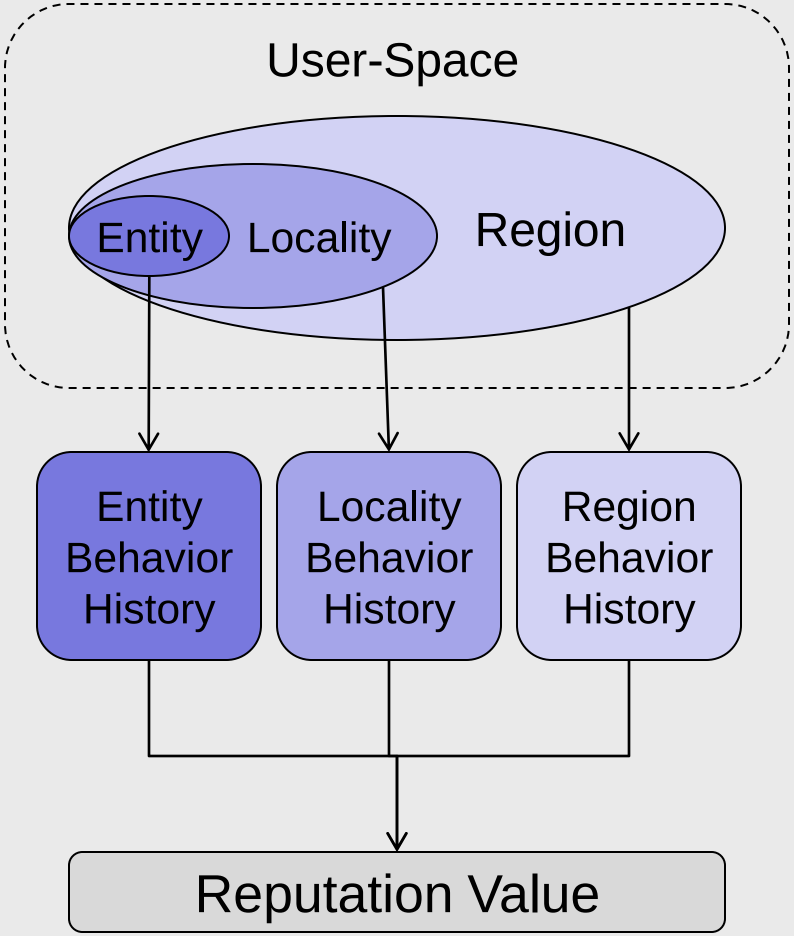
- Develop and harden policy languages and mechanisms for
  - dynamic, multi-layered, fine-grained access control
  - sophisticated control of delegation
  - logic for reasoning with uncertainty
  - logic for reasoning with degrees of trust
- Refine architecture and system further
  - Explore performance/scalability, effectiveness, overhead tradeoff

RTM: Extensions to RTM

- Compute reputations in the context of
  - correlations between corrupted nodes (shared bad files, for example)
  - adversary (BOT Master) recruiting nodes dynamically
  - collusion between bad nodes
  - targeted attacks by bad nodes

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



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?

Integration into QTM

- **New insight:**
  - Computation of the trust value on the TDG has a straightforward mapping to Datalog query evaluation
- NDlog (Network Datalog) is a novel system for distributed query evaluation that can provide a platform for efficient QTM systems
- Future tasks:
  - NDlog encoding of TDG evaluation
  - Integration with reputation databases

QTM: “permission to speak”

- L_{PS} can be used as an alternative to Keynote in the QuanTM architecture
  - – L_{PS} evalutation is based on a logic programming framework
- **New insight:**
  - – Tighter integration with NDlog-based QTM will yield more efficient policy evaluation
- Future tasks:
  - – Define quantitative semantics for L_{PS}
  - – Implement NDlog-based L_{PS} access control

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)

Applications of QTM

- SIE (Security Information Exchange)
- BGP (Border Gateway Protocol)
- CPS (Cyber Physical Systems)
- Cloud Computing

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

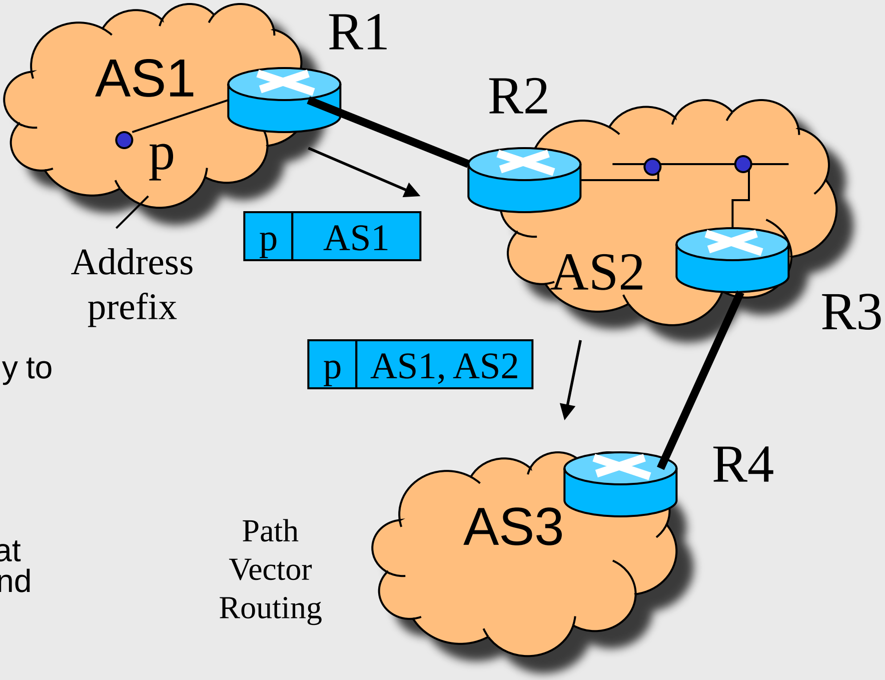
Securing BGP

- Protocol for exchanging information between Autonomous Systems (AS) on how to reach specific destinations. Based on exchange of IP Prefixes
- Acceptance of BGP update packet and forwarding it depends upon custom policies

- Principal vulnerability of BGP – it does not check if:
  - Router introducing prefixes own them
  - Router is using the AS number allocated to it

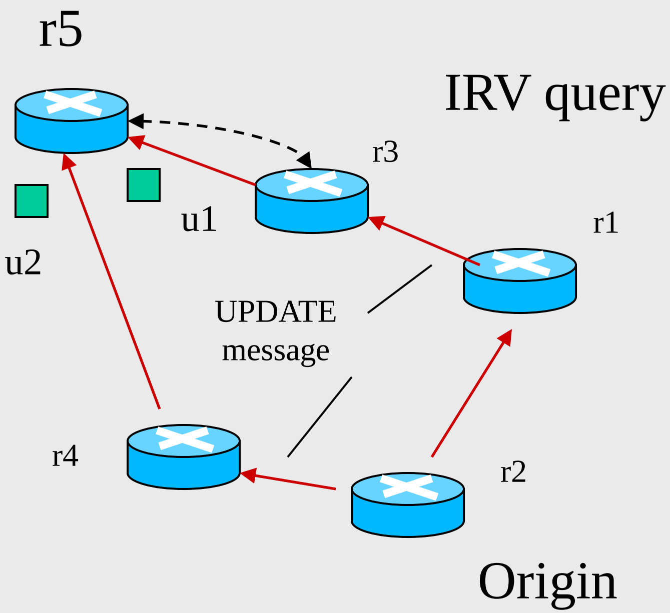
- Current approaches for securing BGP
  - Approach1:
    - Use PKI in the prefix address allocation hierarchy to bind as prefix to AS and AS to organization
    - Expensive (signature and validation needs) and modified BGP
  - Approach 2:
    - Use inter-domain route validation servers (IRV) at ASes which can be used to query the address and path associations
    - IPSec based communication security

- Given the flexibility provided by the policy space in BGP, network-level security is not sufficient – as there is not way to prevent router misbehavior at the policy level



QTM-BGP

- Goal
  - Use QTM to secure BGP without modifying BGP
- Potential Approach
  - Add trust and reputation to BGP policy specification
  - Compute reputation of BGP update (e.g., u1, u2) based on reputation of AS in the path
  - Compute AS reputation (e.g., r1, r2, r3, r4) based on
    - feedback obtained from IRV (Interdomain Route Validation) query mechanism
    - receiver's own experience of past behavior
- Experimental platform
  - Coding QTM-BGP on declarative network simulation toolkit RapidNet (uses Datalog like language) for prototyping



Rep (u1) = fn (r2,r1,r3)
Rep (u2) = fn(r2, r4)

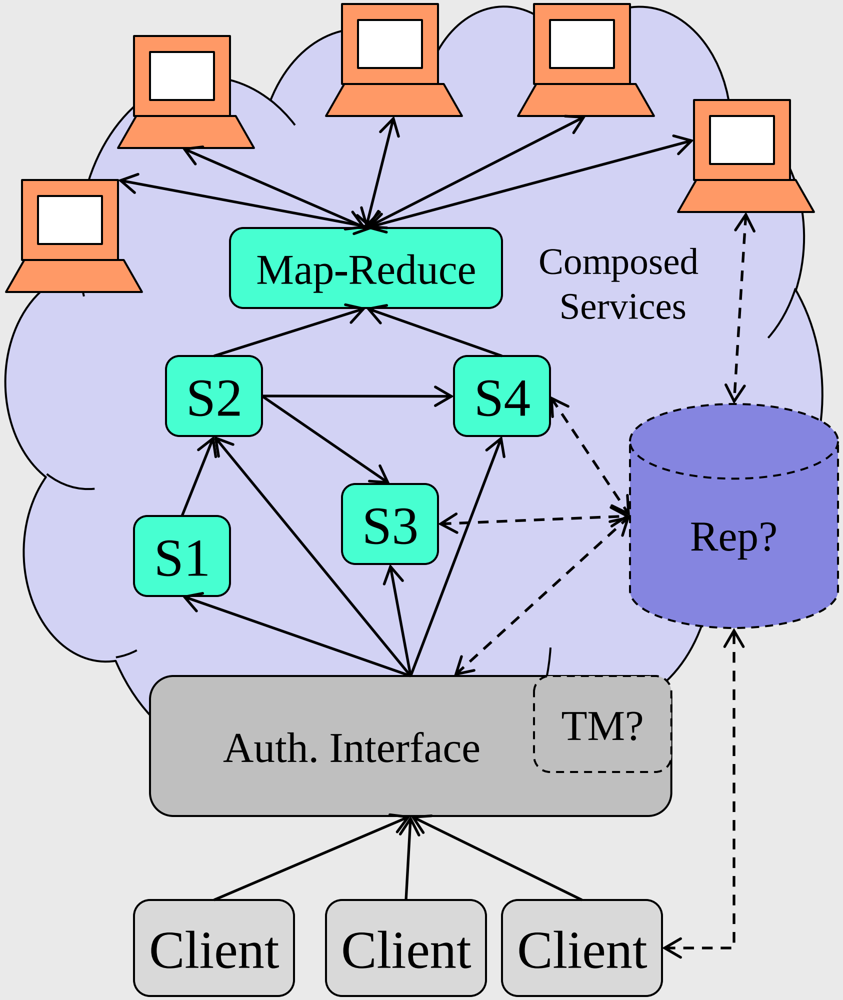
@r5 choose
<u>max</u> (Rep(u1), Rep(u2))

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 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?
  - High level of feedback sharing and density = greater accuracy.
  - Persistent ID: 1 client, many services



THANK YOU!