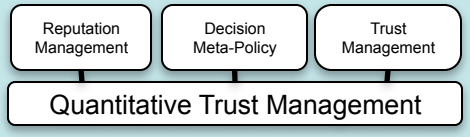
FY09: Foundational and Systems Support for Quantitative Trust Management (6.1 MURI)

Revolutionary Research . . . Relevant Results

STATUS QUO

- ***Trust Management (TM):*** **Cryptographic delegation of access rights between principals using policies and credentials.**
  - **Can't accommodate uncertainty or partial information. Static.**
- ***Reputation Management (RM):*** **Principals hold quantitative opinions of others that change dynamically based on runtime behavior. Opinion strength determines permissible actions.**
  - **Reputation is non-transferrable (no delegation) and lacks an enforcement mechanism.**

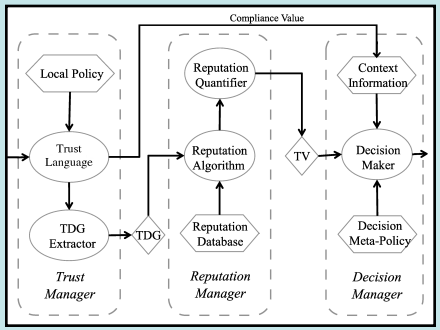
NEW INSIGHTS



- **Selective merging of TM and RM concepts = Quantitative Trust Management (QTM).**
- **QTM can enforce delegated policies *and* adapt that policy as partial information becomes more complete.**
- **Big idea: <u>HOW much should a policy-based decision be trusted given the reputations of the entities involved?</u>**

GAPS

- Outside of specialized-domains, no attempt has been made to hybridize TM and RM systems, which each have their own unique approach to service protection / access control.



At left: Expected component-level workflow of a system applying QTM principles.

We envision QTM systems to be very modular – allowing the plug-and-play of TM languages and RM algorithms.

RESEARCH CONCENTRATION AREAS

- Specifying a data-structure to encode trust dependencies, which remains fixed whatever TM language (*i.e.*, KeyNote) is employed.
- Designing an algorithm which produces a characterizing *trust value* for an access request per the reputations of the parties involved.
- Determining how such *trust values* may combine with the output of TM language evaluators to produce final access decisions (*i.e.*, a new meta-policy language may need written).
- Finding QTM applications – Where are there delegation hierarchies with partial information?

QUALIITATIVE IMPACT

- ***Credential revocation*, a long standing difficulty of TM systems, may be achievable via reputation techniques.**
- **Systems currently utilizing TM could gain flexibility in policy interpretation without having to re-author policies or re-issue credentials.**
- ***Enables a well-defined authorization hierarchy, yet is flexible enough to ignore it under extra-ordinary circumstances (e.g. a national crisis) .***

END-OF-PHASE GOAL

GOAL

- The development of quantitative trust management capability for service-oriented architecture.

FUNDING

FY08 FY09 FY10 FY11 FY12

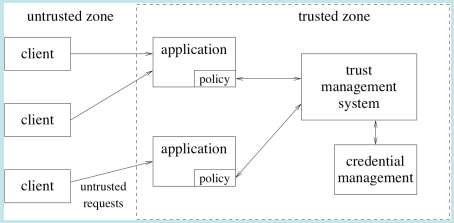
04/01/09

Combining trust and reputation management to enforce *dynamic* access-control policies

Dynamic Trust Management

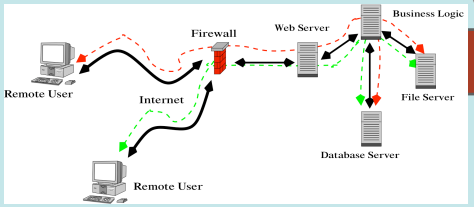
Revolutionary Research . . . Relevant Results

STATUS QUO



- ***Proposed DoD/IC Global Information Grid is a service oriented architecture (SOA) for which simplistic red/black separation is insufficient***
- ***There are a wide range of emergent cyber threats (e.g., botnets) which threaten SOAs***

NEW INSIGHTS



- ***New cooperative and dynamic policy evaluation may permit functioning through challenges such as dynamic service availability in complex SOAs, as well as complex situational dynamics, e.g., attacks on dismounts vs. on base.***

GAPS

- Credential-based authorizations are static, and revocation is hard, while real-world authorizations are dynamic, for example due to dynamic service availability, and require changes based on policy
- Situational dynamics, such as changing network conditions (e.g., botnet attack) or changing kinetic conditions (e.g., mortar attack) are not capable of being addressed
- There is no way to specify continuua of trust (such as reputation) for the the authorizer and authorization chain

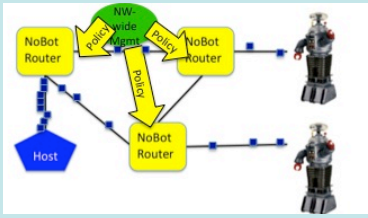
RESEARCH CONCENTRATION AREAS

- Develop new dynamic policy evaluation architecture which provides situation-aware access control and resource control authorization
- Fast scalable revocation schemes
- New algorithms for cooperative and decentralized policy evaluation, for both robustness and fault tolerance
- Update Keynote syntax to reflect CPE/DPE and the addition of reputation evaluation

ASSUMPTIONS

- Availability of strong cryptography and a policy expression language to specify policy
- Availability of reputation information for authorizers and signers

QUALIITATIVE IMPACT



- ***Flexible and robust control of authorizations in complex distributed systems such as the DoD/IC GIG***
- ***The ability to define policies to allow scalable decentralized defense against emergent cyberthreats by rapid adaptation of resource access limits***

END-OF-PHASE GOAL

GOAL

- Define a more mission-based access control model suitable for the GIG.

FUNDING

FY08 FY09 FY10 FY11 FY12

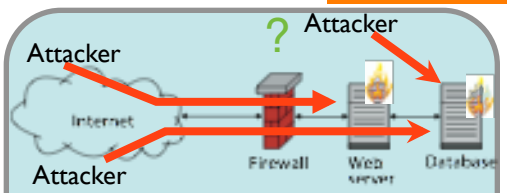
04/01/09

New dynamic TM strategy allows situation-dependent credential-based authorization

FY09 BRC: Coordinated Policy Enforcement in SOAs

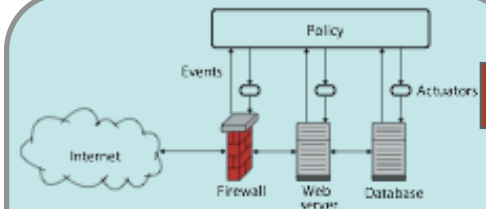
Revolutionary Research . . . Relevant Results

STATUS QUO



- ***Cyber-defenses within and across collaborating enterprises operate without coordination***
- ***Security policies have hidden assumptions***
- ***example: traffic reaching the database was inspected by the firewall and the web server***
  - ***violation: attacker accesses database through unauthorized wireless access point***
- ***Attackers can attack each system component in isolation***

NEW INSIGHTS



- ***Eliminate assumptions by exchanging information among security enforcement mechanisms***
- ***Policy enforcement across an enterprise based on current global information***
- ***Exploit advances in trust management mechanisms***
- ***Allows integration of wide variety of security mechanisms (honeypots, intrusion detection, reactive defenses, etc.)***

GAPS

- Means for effectively expressing intra- and inter-enterprise global security policies
- Insufficient theoretical knowledge of the types of policies that can and cannot be realistically enforced with this new paradigm
- For large/busy enterprise networks, it is unknown how the approach scales with the number of security mechanisms present and the volume of security-critical events that must be examined within the global context
- Means to reason about global events in the context of a local security policy decision

RESEARCH CONCENTRATION AREAS

- Develop prototypes integrating a variety of different, diverse security mechanisms and policy expression methods
- Determine the effectiveness and scalability of the approach via a series of experiments in simulated and real enterprise environments
- Develop fundamental understanding of the tradeoffs between extent of global context, scalability, and ease of defining global policy through scenario-based experimentation
- Investigate appropriate reactive mechanisms that can be leveraged through proposed paradigm
- Determine trust extension techniques for inter-organizational collaboration at the transaction level

ASSUMPTIONS

- Security mechanisms operate under unified administrative control

QUALITATIVE IMPACT

- **Developed 3 prototypes based on different tradeoffs of threat model and extent of global information context**
- **Preliminary experiments show effectiveness in preventing attacks that could not be previously averted**
- **Performance impact currently noticeable but small for one prototype, high for another**
- ***Enabling intelligent cyberdefense-in-depth in mission-critical systems, with an emphasis on web-based Service-Oriented Architectures***

END-OF-PHASE GOAL

GOAL

- Consistent, continuous, assumption-free security policy enforcement across distributed enterprise

FUNDING

FY08 FY09 FY10 FY11 FY12

04/01/09

New paradigm for unified security policy enforcement across a distributed enterprise network

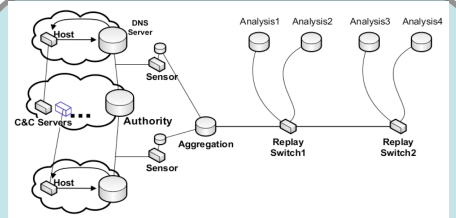
FY09: Foundational and System Support for Quantitative Trust Management

Revolutionary Research . . . Relevant Results

STATUS QUO

- *Computers on the Internet can be compromised and become "bots"*
- *Botnets are responsible for most of the large-scale attacks and fraudulent activities on the Internet*
- *Network monitors employ a list of known domains used for botnet command-and-control (C&C), a list of known bots. These are "untrustworthy" hosts. The information is "dynamic"*
- *There is very little sharing among the security vendors*
- *Threats change faster than product updates*

NEW INSIGHTS



- *More comprehensive and accurate understanding of botnet threats can be obtained only if more data is available*
- *Security vendors and network operators are willing to share local findings if they can benefit from the aggregate/ global analysis*

GAPS

- Means to determine what, where, and how many sensors (data contributors) are needed to provide a comprehensive analysis of specific botnet threat, including its population, growth trend/ patterns, and attack patterns
- Means to exploit sampling to achieve optimal analysis results in the face of very large volume of streaming data
- Means to dynamically score the "trustworthiness" of a host based on analysis results

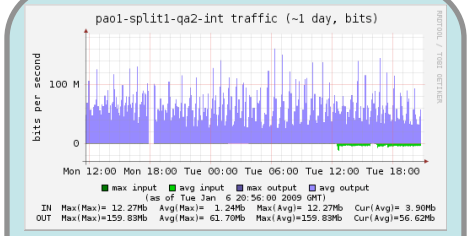
RESEARCH CONCENTRATION AREAS

- Develop theoretical understanding and models of botnet C&C and operations to guide the optimal deployment of sensors
- Develop fundamental understanding that lead to practical sampling and analysis (e.g., clustering) algorithms that support real time analysis of streaming data
- Develop mathematically sound scoring models that combine multiple factors, including temporal information.

ASSUMPTIONS

- There is no privacy violation for sharing local security findings (e.g., who attacked our networks, where is the bot traffic directed to)
- Sufficient "infrastructure/equipment" funding for sensors and analysis servers

QUALIITATIVE IMPACT



- **Sensor deployment covers at least the networks of North America; the goal is the Internet as much as possible**
- **Analysis on aggregate data more comprehensive, accurate, and timely than any local network (even a large ISP) alone can obtain**
- **Sustained deployment and maintenance to counter threats of future malicious overlay networks**

END-OF-PHASE GOAL

GOAL

- Enabling a new paradigm for data sharing and analysis to provide accurate and dynamic Internet trust information

FUNDING

FY08 FY09 FY10 FY11 FY12

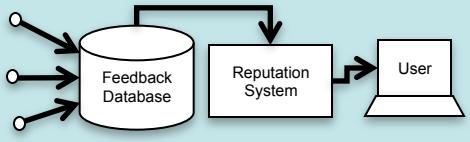
04/01/09

New strategy to share data and analysis to counter botnet threats

FY09: Comparing/Composing Robust Reputation Systems

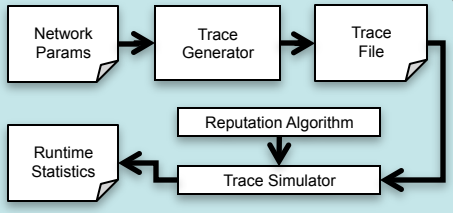
Revolutionary Research . . . Relevant Results

STATUS QUO



- ***Reputation system:*** **Dynamically uses interaction history as basis for predicting future conduct.**
- ***No direct experience?:*** **Selective use of other's personal histories creates a reputation network.**
- ***Systems/algorithms in existence:*** **TNA-SL, EigenTrust, eBay (often rooted in statistics, fuzzy logic).**

NEW INSIGHTS



- **By comparatively analyzing reputation algorithms' handling of malicious behavior, fundamental features of effective systems can be identified.**
- **Composing these features, a highly effective reputation system can be constructed.**

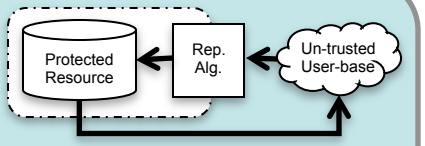
GAPS

- Comparative analysis has not been performed on existing reputation systems, due-in-part to the lack of a general-purpose evaluation framework.
- Differing assumptions made by systems complicate construction of an objective test-bed.
- Production of interesting test traces is difficult given the decentralized nature of many applications and the subjective nature of feedback.
- Theoretical systems, while claiming robustness, often give no consideration to scalability

RESEARCH CONCENTRATION AREAS

- Designing and constructing an objective framework for testing reputation systems under varying network conditions and against diverse malicious user/collective strategies.
- Determining attack strategies most effective (*i.e.*, devastating) against current systems, so future systems may avoid such vulnerabilities
- Improving reputation algorithm scalability using heuristics and incremental calculation.
- Producing realistic reputation network traces based on empirical studies and intuition.
- Optimizing program variables (*i.e.*, thresholds, bounds) for efficiency and effectiveness.

QUALIITATIVE IMPACT



- **Composition of robust alg. features will produce a new, stronger reputation system.**
- **Demonstrated effectiveness, combined with flexibility via feedback, will make our system a viable choice for protecting increasingly critical resources.**
- ***Enabling systems currently monitored by static trust systems to be complemented or replaced by dynamic reputation ones***

END-OF-PHASE GOAL

GOAL

- The design of a more efficient, effective, and secure reputation system

FUNDING

FY08 FY09 FY10 FY11 FY12

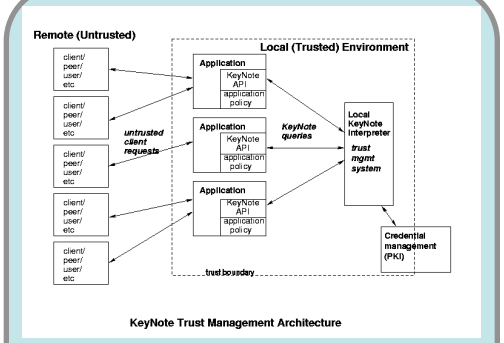
04/01/09

Comparative analysis of existing reputation algorithms will aid future design attempts

FY09: Towards Trust Management in Service-Oriented Architectures

Revolutionary Research . . . Relevant Results

STATUS QUO



KeyNote Trust Management Architecture

- ***Access control methods evaluate compliance with respect to a single policy***
- ***Single source of authority is assumed***

NEW INSIGHTS

- ***Security policies may be introduced independently by individual service providers in an SOA***
- ***Deontic modalities offer explicit representation of permission and obligation***
- ***Interplay between delegation of authority and imposition of obligations can be exposed***
- ***Classical instead of intuitionistic semantics may be possible, improving reasoning efficiency***

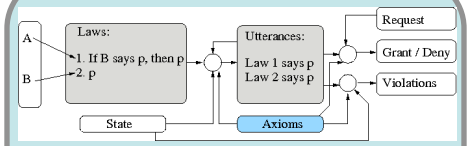
GAPS

- New access control mechanisms are needed to accommodate multiple source of authority in SOA
- Conflicting policies may exist in systems with multiple sources of authority. Conflicts between policies need to be identified. Compliance of a policy to a set of other policies need to be evaluated
- A request for service may affect several service providers. If a request is granted, it needs to be evaluated against all applicable policies.
- If a request is denied, the user needs to be provided with feedback on which policies are violated and why they are relevant to the request
- Permissions and obligations implied by a security policy are left implicit, leading to semantic paradoxes

RESEARCH CONCENTRATION AREAS

- Develop sound and complete access control logics and study their properties
- Develop practical policy languages for distributed security policies based on deontic modalities
- Develop algorithms for conformance checking and blame assignment
- Evaluate decentralized access control using healthcare domain case studies
- Develop sentence-level natural language processing techniques for extracting security policies from regulatory documents

QUALIITATIVE IMPACT



- **Evaluating service requests under multiple authority sources**
- **Detecting conflicts between policies**
- **Relating access control and general policy compliance**
- **Understanding permissions and obligations implied by a set of decentralized policies**
- ***Providing flexible access control for independent service providers***

END-OF-PHASE GOAL

GOAL

- Develop a policy language and compliance mechanism for access control in SOA

FUNDING

FY08 FY09 FY10 FY11 FY12

04/01/09

Combining authorization with deontic modalities for efficient access control in SOA