Information Operation across Infospheres

Prof. Bhavani Thuraisingham
The University of Texas at Dallas

January 2008

Our Approach

- Integrate the Medicaid claims data and mine the data; next enforce policies and determine how much information has been lost (Trustworthy partners)
- Apply game theory and probing to extract information from semi-trustworthy partners
- Conduct information operations (defensive and offensive) and determine the actions of an untrustworthy partner.
- Examine RBAC and UCON for coalitions
- Trust for Peer to Peer Networks

Accomplishments to date

- **FY06: Presented at 2006 AFOSR Meeting**

  - Investigated the amount of information loss by enforcing policies – Considered release factor

  - Preliminary research on RBAC/UCON; Game theory approach, Defensive operations

- **FY07: Presented at 2007 AFOSR Meeting**

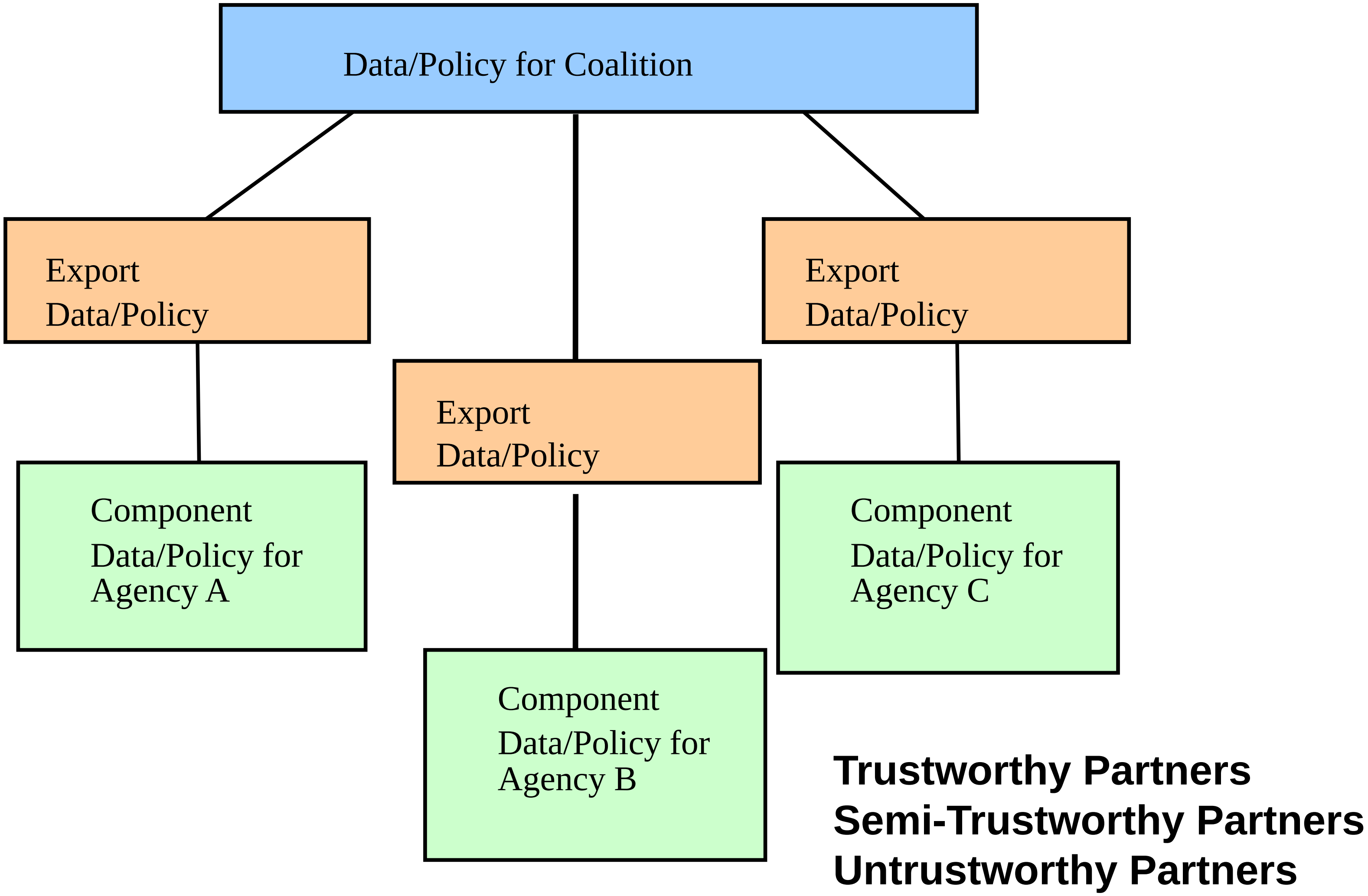
  - Completion of Prototype

  - Solutions using game theory, Penny for P2P Trust, Data mining for Code blocker and Botnet, RBAC/UCON

- **FY08 Plans: To be presented 2008 AFOSR Meeting**

  - Offensive Operations, Prototype integrated system

Technical Details: Architecture



Data/Policy for Coalition

Export Data/Policy

Export Data/Policy

Export Data/Policy

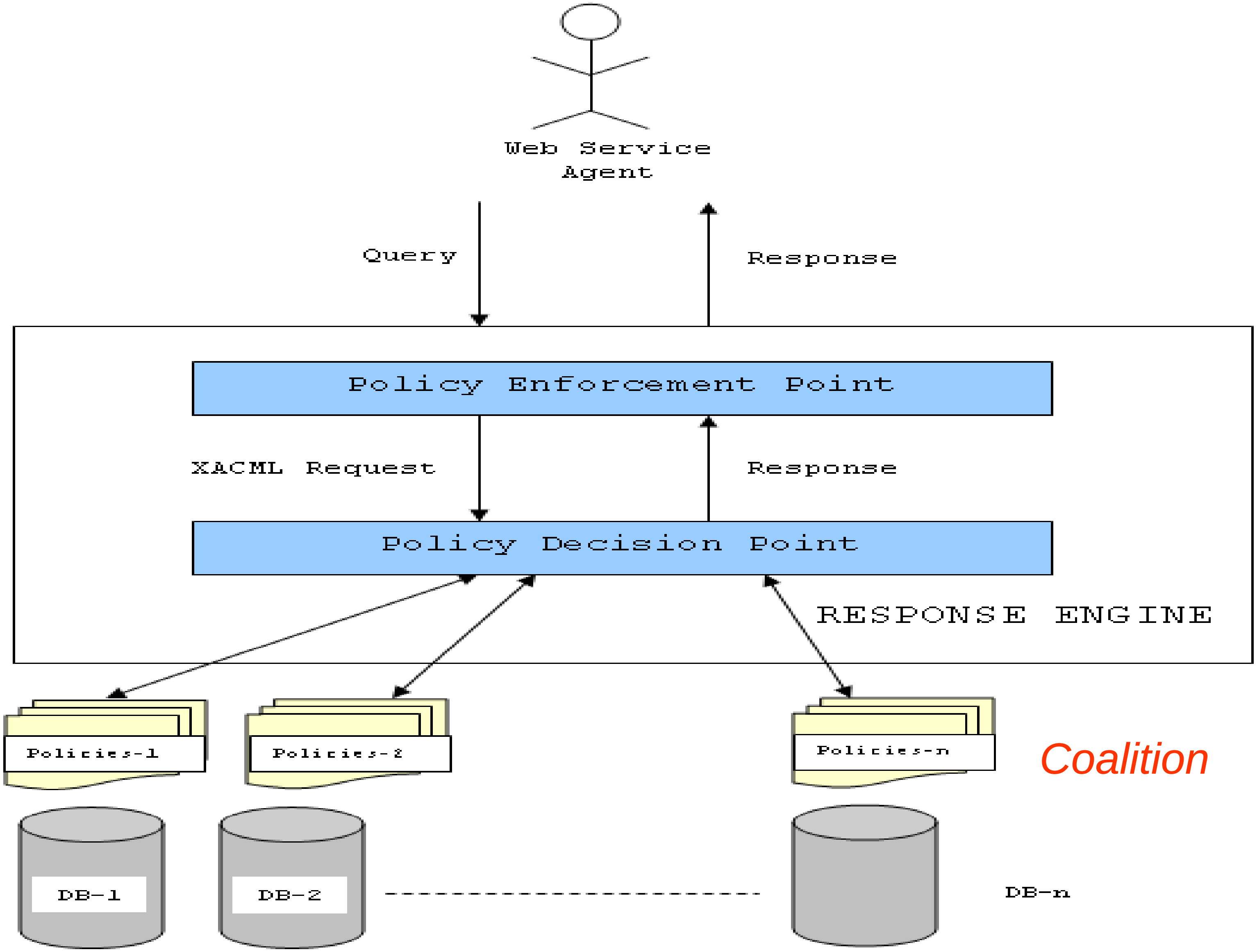
Component Data/Policy for Agency A

Component Data/Policy for Agency B

Component Data/Policy for Agency C

Trustworthy Partners
Semi-Trustworthy Partners
Untrustworthy Partners

Policy Enforcement Prototype



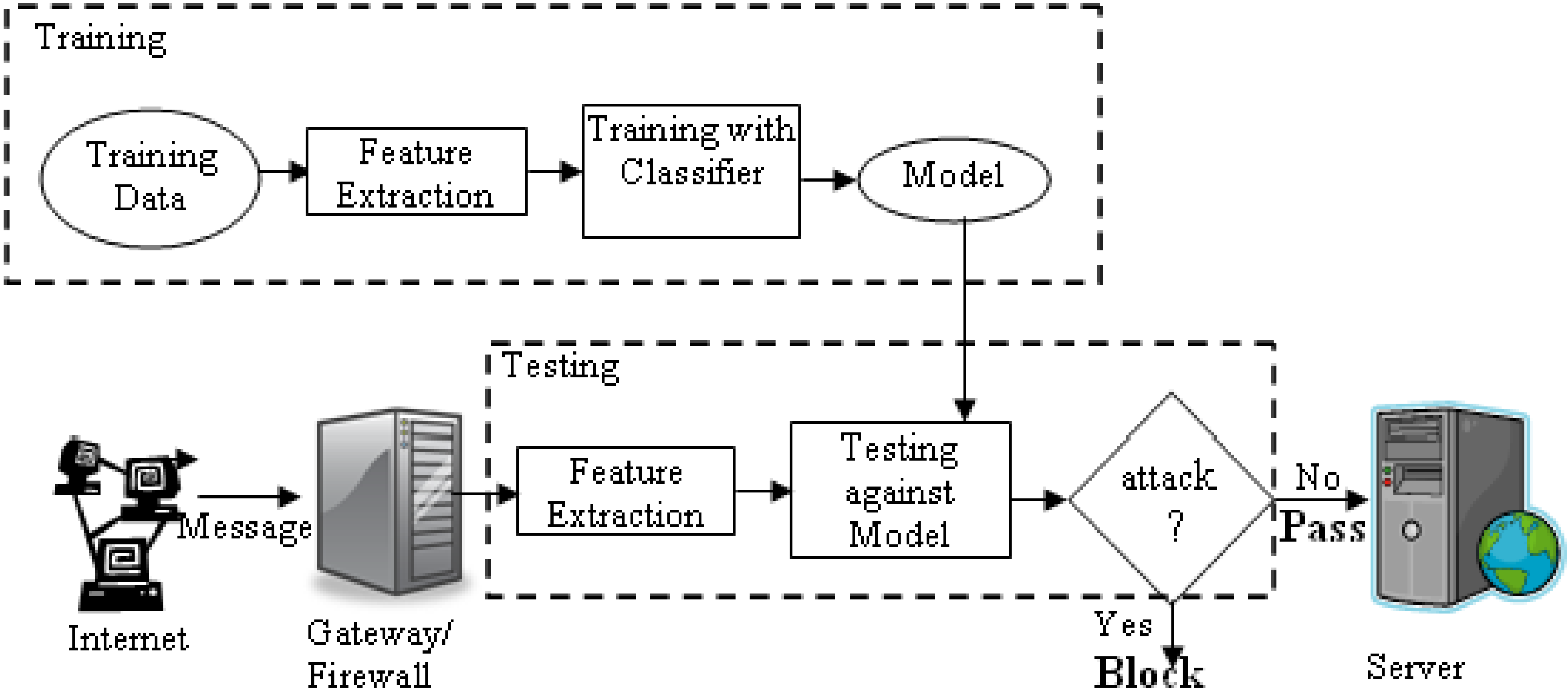
Semi-Trustworthy Partners
Enforcing Honesty

- Everyone has a choice:
  - Tell the truth
  - Lie
- Unless we can afford to have a neutral 3rd party that everyone can agree on, we need some way of enforcing ‘good’ behavior
- However, there is a third option: *refuse to participate*
  - Usually not researched
  - Drastic measure that only makes sense if we can influence behavior
- Our modeling suggests that, with proper use of refusal, we can ultimately enforce helpful behavior without a managing agent

Application of Game Theory

- Every 200 rounds, we create a new generation of agents, using the most successful strategies available
- The fitness *f()* of a given agent is a function of how well they have performed during interaction with other agents
  - More successful agents have a higher probability of being a part of the next generation
- Our mathematical models suggest that, assuming we punish by cutting off communication, the equilibrium is to always tell the truth
- Therefore, using an evolutionary environment, we have placed our particular rationality amongst a heterogeneous pool of competing ideologies
  - **Tit-For-Tat**: A famous algorithm that simply mirrors the last move an opponent made
  - **Random**: An agent that selects it's strategy with a 50/50 chance
  - **Casual Liar**: lies with a 10% probability
  - **Subtle Liar**: chooses to lie when it perceives the piece being traded is of significant value
  - Truthful-punishment: Says the truth; punishes lies by cutting off communication
- With equal parts given to each agent, which one will emerge victorious?

Untrustworthy Partners
CodeBlocker (Our approach)



•Based on the Observation: ***Attack messages usually contain code while normal messages contain data;***
Check whether message contains code
Problem to solve: Distinguishing code from data

UCON Policy Model for Assured Information Sharing

- Operations that we need to model:
  - Document read by a member.
  - Adding/removing a member to/from the group
  - Adding/removing a document to/from the group
- Member attributes
  - Member: boolean
  - TS-join: join time
  - TS-leave: leave time
- Document attributes
  - D-Member: boolean
  - D-TS-join: join time
  - D-TS-leave: leave time

Penny: Trust in P2P Network

- **A P2P Network** that addresses the following types of attacks:
  - Spread of corrupt or incorrect data
  - Attaching incorrect labels to data
  - Discovering which peers own particular data
  - Generating a list of all peers who own particular data
- P2P Network that supports shared data labeling of:
  - Confidentiality
  - Integrity
- Peers can share data without revealing which data object they own
- Security labels are global but do not require a centralized server
- P2P Network uses reputation-based trust management system
  - Store/retrieve labels
  - Despite malicious peer existence
- Maintain efficiency of network operations
- O(log N)

Publications and Plans

- Some Recent Publications:
- Assured Information Sharing: Book Chapter on Intelligence and Security Informatics, Springer
- Simulation of Trust Management in a Coalition Environment, Proceedings IEEE FTDCS, March 2007
- Data Mining for Malicious Code Detection, Journal of Information Security and Privacy, Accepted 2007
- Enforcing Honesty in Assured Information Sharing within a Distributed System, Proceedings IFIP Data Security Conference, July 2007
- Centralized Reputation in Decentralized P2P Networks, IEEE ACSAC 2007
- Malicious Code Detection, IFIP Digital Forensics Conference, January 2008
- Plans:
- Offensive Operations – find out what our untrustworthy partners are doing
- Integrated prototype – partners will change trust levels
- Scenario developments for prototype demonstration
- Technology Transfer to commercial products; operational programs

Why Should AFOSR fund this Research

- Joint Battlespace Infospheres (JBI) is a term coined by the AFSAB
- Assured Information Sharing is central to the JBI as well as migrating toward a need to share paradigm
- We believe that the Air Force is a leader in Data security and Information management and this project will bring the two areas together
- Through this research the AF can lead the DoD as well as DISA/NSA in Network Centric Enterprise Services as well as the Global Information Grid
- Handling partners at different trust levels is a unique contribution made by this project and will have a significant impact on the way the AF and DoD collaborates with its allies as well as with partners they need to collaborate with to support the war fighter

Collaboration

- Project Partners:
  - University of Texas at Dallas
    - **Profs. Latifur Khan, Murat Kantarcioglu and Kevin Hamlen**
  - University of Texas at San Antonio
    - **Prof. Ravi Sandhu**
- Research results were used to prepare the one page for DoD/AFOSR MURI and we have subsequently submitted a proposal in collaboration with UMBC, Purdue, UIUC, U of MI and UTSA
- We will utilize the research results in a DoD project we hope to start on Secure Information Grid
  - We also plan to discus the progress made on the grid project with DOE
- We are discussing with other agencies (e.g., IARPA) to apply the research results into their Blackbook Environment
- Research is directly applicable to DISA/NCES and NSA/GIG