Game Theoretic and Utility-Based Security in MP2P

Brent Lagesse & Mohan Kumar
Dept. of Computer Science Engineering
University of Texas -- Arlington

Brent.Lagesse@uta.edu

Motivating Example

Perspective

- Bootstrapping
- Routing
- Resource Access
- Resource Access Control

- This talk is about Resource Access

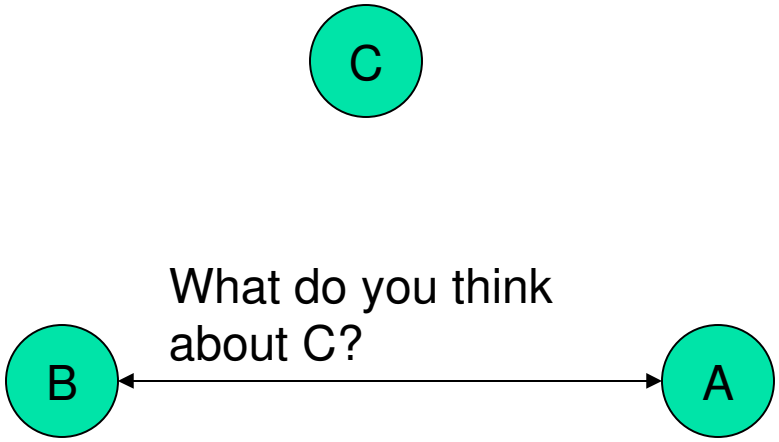
Security in Context

- Malicious peers
  - Serve faulty resources
  - DoS
  - Steal information
- Benign peers may be unreliable

- In this context, security means being able to get what we want, when we want it

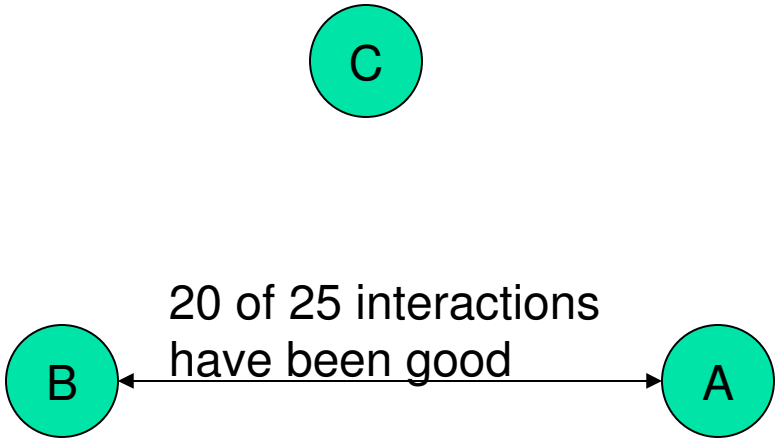
Reputation

- Most common solution
- A cooperative effort
- Peers pass reputation information to each other describing previous transactions



Reputation

- Most common solution
- A cooperative effort
- Peers pass reputation information to each other describing previous transactions



Reputation

- Advantages
  - Many mechanisms are very effective against small number of attackers
- Disadvantages
  - Fails when most peers are malicious
  - Susceptible to startup attacks and one-time attacks
  - Fails when assumptions do not hold

System Goal

- Using reputation is difficult in some situations
  - Uncertain/Malicious systems
  - Systems with intermittent connectivity
  - Systems with peers that are very sensitive to attack
- Goal: Provide protection for peers in systems where reputation performs poorly

Utility Model

Utility =

- *Benign Benefits + Malicious Benefits*
- *– (Benign Costs + Malicious Costs)*
- *– Victim Costs*
- *– Discovery Costs*

Benign Benefits

Benefit from Access To Resources

Benefit from Mechanisms (ie incentives)

Malicious Benefits

Benefit from Spying on Access

Benefit from Denying Access

Benefit from Misinforming the User

Utility Model

Utility =

- *Benign Benefits + Malicious Benefits*
- *– (Benign Costs + Malicious Costs)*
- *– Victim Costs*
- *– Discovery Costs*

Benign Costs

Cost of being in the system

Cost of providing Resources

Cost from mechanisms (ie, payments)

Malicious Costs

Cost of Spying on Access

Cost of Denying Access

Cost of Misinforming the User

Utility Model

Utility =

- *Benign Benefits + Malicious Benefits*
- *– (Benign Costs + Malicious Costs)*
- *– Victim Costs*
- *– Discovery Costs*

Victim Costs

The cost incurred as a result of being a victim

Discovery Costs

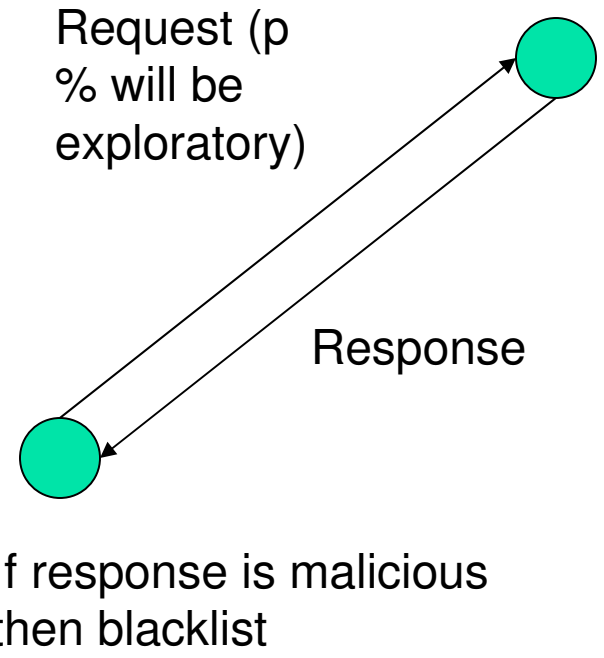
The costs incurred as a result of being discovered as an attacker

Modeling Peers

- Purely Malicious
  - Malicious Benefits, Benign Costs, Malicious Costs, Discovery Costs
- Purely Benign
  - Benign Benefits, Benign Costs, Victim Costs
- Hybrid Malicious/Benign
  - All components

Resource Exploration

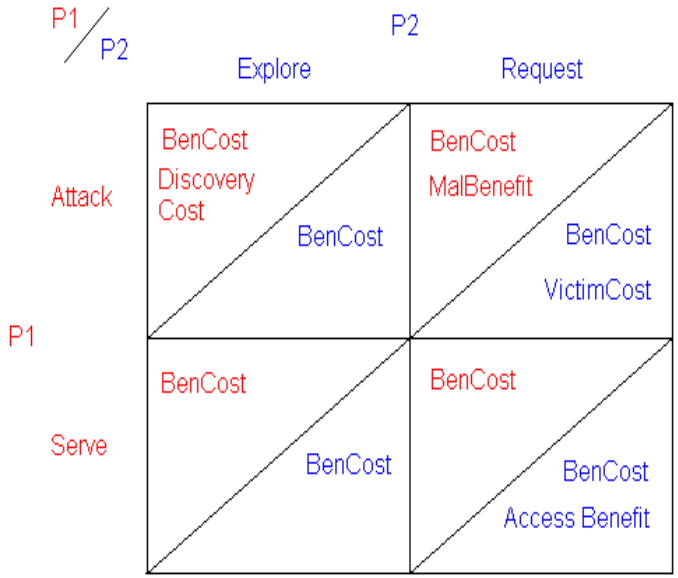
- Send a mixture of *p%* exploratory and *(100-p)%* real requests
- Effect
  - Increased number of Benign Costs
  - Decreased number of Victim Costs



How to choose p?

- Game Theoretic approach
  - Requires more knowledge than we will probably have
- Utility bounded
  - No guarantees, but at least tells us what to e

ResExp Payoff Matrix

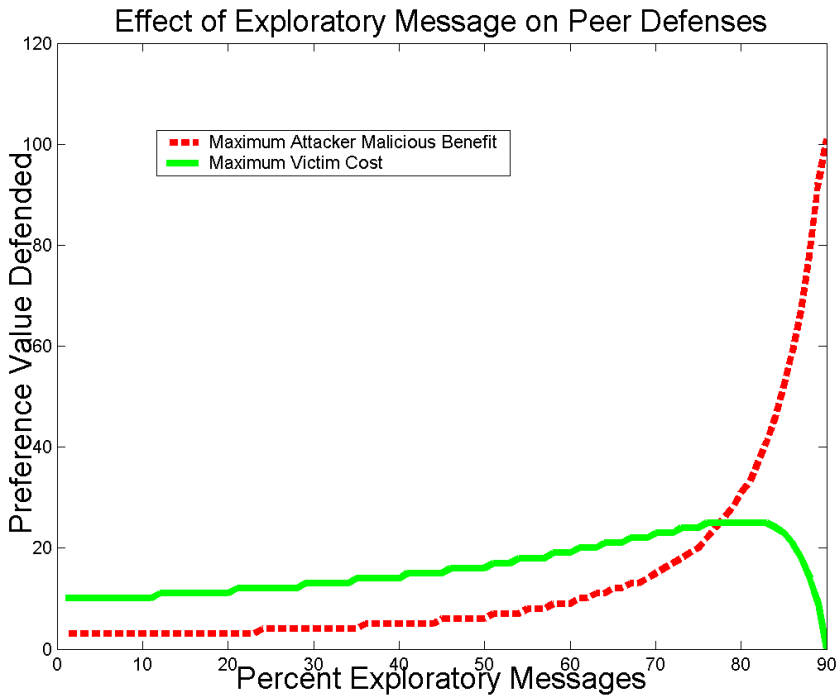


$$P_{exp} = \frac{MaliciousBenefit}{DiscoveryCost + MaliciousBenefit}$$

$$P_{attack} = \frac{BenignBenefit}{VictimCost + BenignBenefit}$$

Utility Bounds

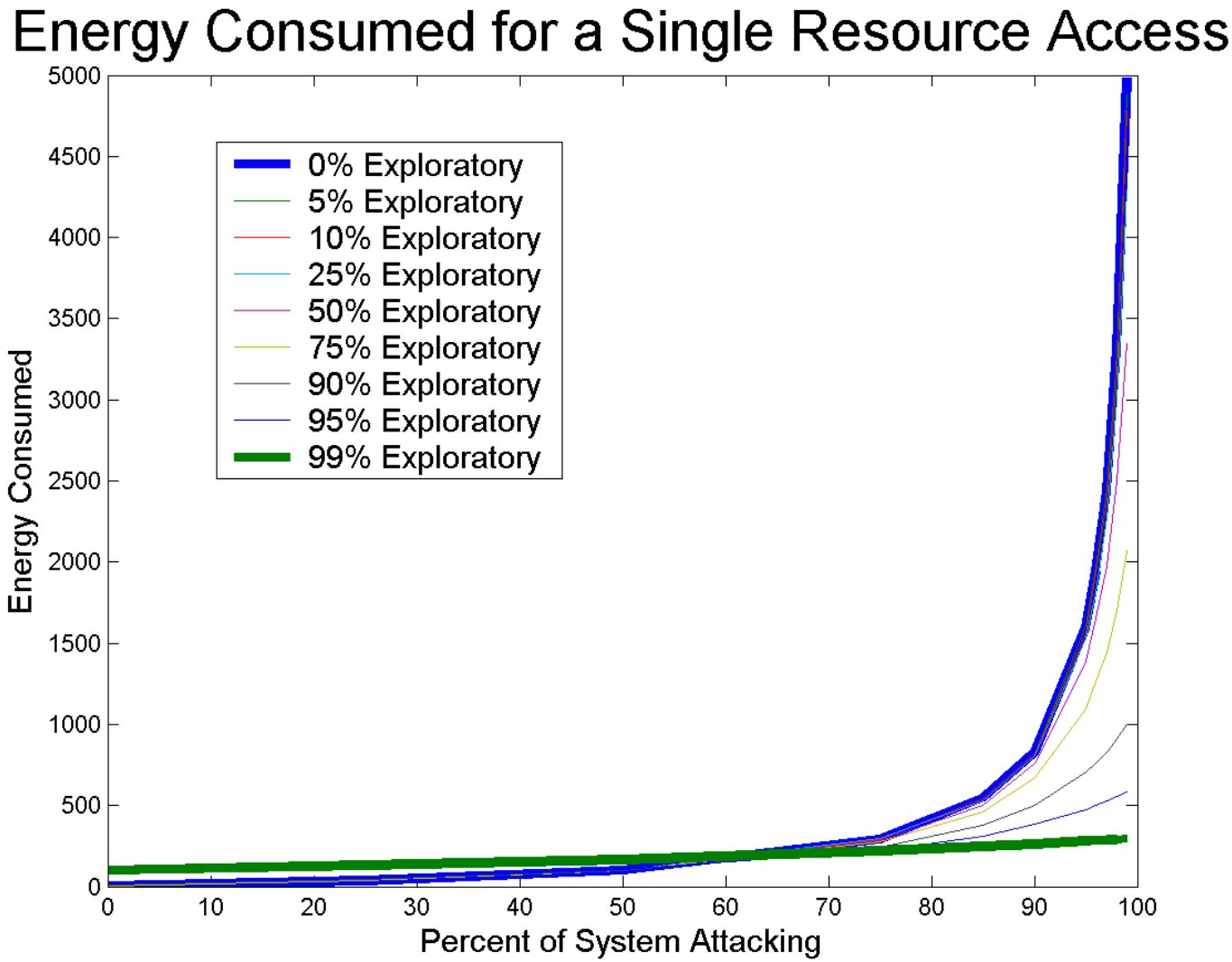
- Only if the attacker's preference for attacking is above the **red line**, it is rational for it to attack
- Only if the benign peer's cost of being a victim is below the **green line** is it rational to participate in the system



Energy Considerations

Benign Costs = 1

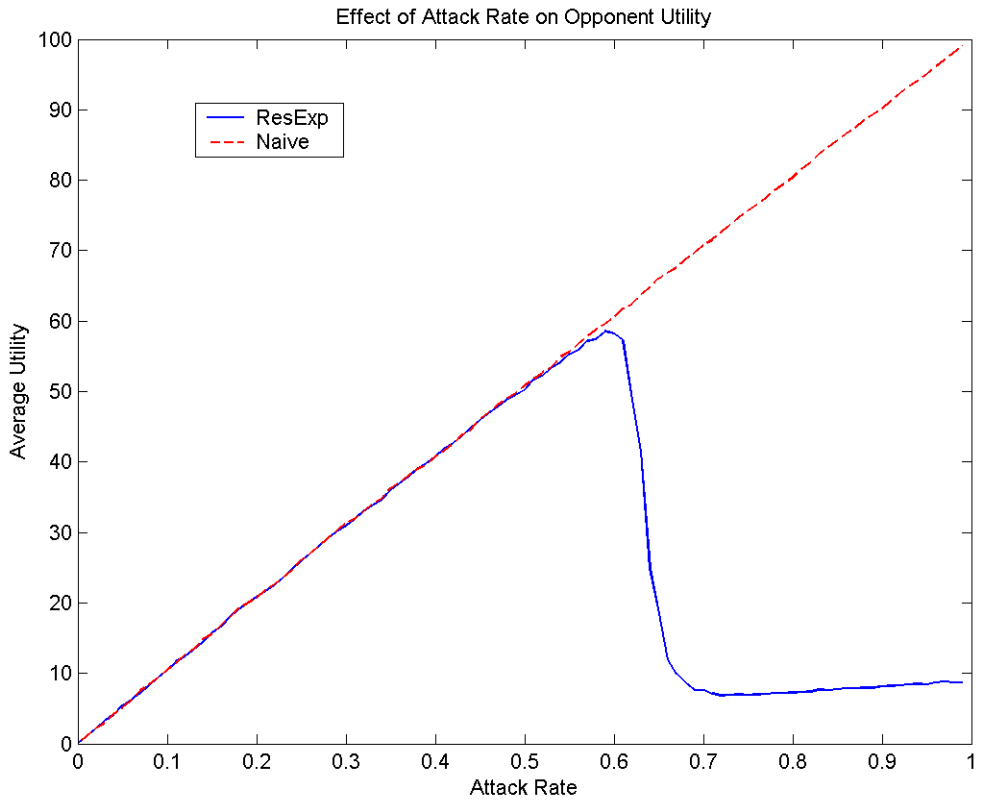
Victim Costs = 100



Effect of Attack Rate on Opponent Utility

Benign Costs = 1

Malicious Benefit = 100



- Attacker always attacks against naïve user, only 62% of the time against ResExp user

Conclusions

- Defined a utility model for peers
- Introduced Resource Exploration
  - Works well in malicious and uncertain environments
  - Scales well with respect to percentage of malicious peers
- Currently designing and testing Resource Exploration and in many environments