CFP Announcement: CIP Call for Proposal  
Mission Area: Intrusion Response System  
Proposal Title: Response to Collaborative Attacks Against Network Vulnerability  

Problem Scenario

Operational Capability to be Provided:

- Atomic attack can be detected using Extended attack graph which captures normal and anomalous patterns in a form of graphs. Capturing all the individual actions as patterns and combining these actions will help us to identify co-operative anomalous actions.
- To allow the domain specialist to analyze the joint pattern in a meaningful way and detect existing vulnerabilities in the system.
- IBM Internet Security Systems (ISS), CISCO support similar research in vulnerability management.
- NSF and DOD have Call For Proposal (CFP) in this new and important area.

Proposed Technical Approach: New Approach

Task 1:
- Survey and investigate current intrusion response solutions (e.g. preemption based, tracing based, attack graph based) for attack planning and vulnerability analysis of a network of hosts.
- Study and evaluate how well the existing and new response solutions can be applied to the above distributed environment.

Task 2:
- Design a new automated response solution for the distributed environments by extending preemptive response solution for a single host. The mechanism will provide to respond against global vulnerability due to sequential and concurrent atomic attacks in a network.
- Testing the response mechanism using simulation/prototype implementation in a distributed environment.

Cost & Schedule:

- Task 1 period: 3 months; Task 2 begins after the completion of Task 1 for a period of 9 months.
  - Total Period of Performance is 12 months
- Task 1 - Cost of $5,000
- Task 2 - Cost of $20,000;
  - Total Cost is $25,000

Deliverables

- Technical report describing model and techniques to build the solutions for a network of multiple hosts (distributed environment).
- Software prototype or simulation model of the secure system will be built and make available to CIP members.

Departmental Information:

- Johnny Wong, Samik Basu, Department of Computer Science, Iowa State University, Ames IA 50011
- Email: [wong, sbasu]@cs.iastate.edu