Adaptive Threat Management Tool for Cyber-based Systems
Yahya Javed, Tawfeeq Shawly, Muhammad Felemban, and Arif Ghafoor
URL (http://multimedia.ecn.purdue.edu/AIMS.html)

Objective: Develop resilient Cyber-based System (CBS) by incorporating an adaptive threat management mechanism throughout the life cycle of such system from design through recovery from cyber attacks.

System Architecture

System Components
1. Intrusion Detection
2. Intrusion Boundary (IB) Manager
   - Damage confinement
   - Scalability
3. Threat Response
4. CBS Recovery

Proposed Solutions
1. Adaptive Intrusion Management System (AIMS) for big datacenters
2. Adaptive Threat Management (ATM) for CBS

AIMS
Solution Methodology
1. IB demarcation as a metrics-driven optimization problem for damage confinement
2. Development of an efficient intrusion response and recovery mechanism for malicious transactions
3. Development of malicious workload benchmarks for performance evaluation

ATM
Solution Methodology
1. Development of a real-time HMM-based intrusion detection
2. Development of firewall policy-based response and recovery playbook
3. Development of a risk-aware partitioning mechanism for scalable detection, response, and recovery
4. Development of an ATM prototype for testing and validation

Acknowledgement: This work is supported in part by a grant from the Northrop Grumman Corporation and National Science Foundation Grant IIS-0964639.