MASTERS
FINAL ORAL EXAMINATION

Wednesday, November 9th
3:00p.m. @ 223 Atanasoff

Maheedhar Gunasekharan

Major Professor: Samik Basu

A Framework for Selecting the Minimal Set of Preferred Responses to Counter Detected Intrusions

Over the past decades, cyber attacks have grown in frequency as well as in sophistication. Often, they elude the counter-measures that are in place due to inadequate expert man-power that is necessary to manually deploy the correct responses and maintain systems being compromised. We present a decision support framework to aid in timely deployment and maintenance of effective responses when intrusive or malicious behavior is detected.

The support framework has two specific objectives: to identify the best set of responses given the knowledge of the attack and the system being protected; and to identify the minimal set of responses that must be deployed. While appropriateness of responses is of utmost importance to safeguard systems from attacks, minimality in the number of responses, an important factor from the deployment and maintainability perspective, has often been discarded. Our framework leverages National Vulnerability Database as a source for information about the attacks, relies on the pre-specified expert knowledge about the responses that can adequately stop attack and takes into considerations the impact of an attack as well as responses on the system being protected in terms of well-studied CIA (Confidentiality, Integrity and Availability) vector.

We investigate and evaluate several heuristics with the goal of searching part of the potentially large solution space and compute a solution that is "close" to the optimal solution. We discuss the relative advantages and disadvantages of each heuristic, and present a specific one that is efficient in computing the optimal solution.

IOWA STATE UNIVERSITY
Department of Computer Science