Faculty of Computer Science UNB

Faculty of Computer Science 2007-2008 Seminar Series

A framework for an adaptive, cost-sensitive intrusion detection and response system

By

Natalia Stakhanova

Wednesday, October 3rd, 2007
3:30pm
ITC317

Sophisticated attacks on computer systems are increasing rapidly. When detected, a fast reaction is required to minimize damage. A human administrative response is slow and requires great expertise. We propose an integrated approach to intrusion detection and response based on the technique for monitoring program behavior for abnormal patterns. Our model allows adaptive and preemptive attack detection and deployment of the most effective response strategy determined through a multi-phase response selection mechanism based on the costs of potential intrusion and candidate responses.

★★
STUDENTS ARE ENCOURAGED TO ATTEND
★★