PANICHPRECHA, Sorot
Bsc (Computer Science) Thammasat University Thailand, MInfTech QUT

Thesis Title:
Abstracting and Correlating Heterogeneous Events to Detect Complex Scenarios

Supervisors:
Adjunct Professor George Mohay (Principal)
Associate Professor Andrew Clark (Associate)
Dr Jacob Zimmermann (Associate)

Citation:
The research described in this thesis investigated problems inherent in the specification and detection of multi-step attacks against heterogeneous computer networks and systems. The research developed a model for abstract event representation and a corresponding novel signature-based intrusion detection system to detect multi-step attacks. Several inherent problems in signature-based intrusion detection systems operating in heterogeneous environments have been investigated. The lack of an abstract event model has been addressed by the use of a flexible and extensible event representation that builds on object oriented techniques. The complexity of detecting multi-step attacks has been addressed by an intuitive algorithm. The thesis investigated time uncertainty issues resulting from unreliable event timestamps. Such issues have been previously overlooked by intrusion detection research. The solutions to the time uncertainty issues have been explored and discussed. A prototype of the signature-based intrusion detection system has been developed and evaluated.