University of Macau

Abstract

MINING SUSPICIOUS ACCESS PATTERNS IN SECURE PHYSICAL ENVIRONMENTS

by Yan Pengfan

Thesis Supervisor: Dr. Simon Fong
Thesis Co-supervisors: Dr. Robert P. Biuk-Aghai
Software Engineering

Security in physical environments has become increasingly important in the wake of terror and criminal activity, particularly over the past decade. One of the challenges is to identify activities that may not be outright illegal or breaches of security, but that are suspicious, i.e. where there is a possibility that these activities may lead to breaches of security. Technology such as RFID is used to track the access and movement of people in highly security physical environments. This thesis presents methods of detecting patterns of suspicious activity in logs collected by such physical access control systems. Traditional Intrusion Detection Systems (IDS) are based on matching the characterization of the attack and the tracking of the activities, and moreover data mining can make the appearance in our field. Either existing IDS [1] or SAD for physical world doesn't involve related detection measurement in our field. In this thesis, we have proposed a concrete detection model and develop a real-time suspicious access patterns detection system, which can extract principal features of access pattern and identify suspicious movements.

Keywords: RFID, IDS, security, Data mining, physical environment, Simulation, Real-time, Tracking system, path finding, access event, control system, classification.