

A Comprehensive Reasoning Framework for Information Survivability

S. Upadhyaya, R. Chinchani, K. Kwiat

Presented by: Maria Calle

Information Assurance
PhD Seminar – Summer 2006

Overview

- Authors developed a framework for real time intrusion detection: a CIDS (concurrent intrusion detection scheme)
- Tries to detect "internal" threats:
 - Masquerading (pretending to be another person)
 - Legitimate user penetrations (knowledge of application)
 - Internal abuse (damage or abuse of the resources from inside)
 - Illegal resource access
- No other aspect of Survivability considered
- Intrusion detection is not a binary decision
- Authors use encapsulation of user intent: user must specify what he is going to do at the beginning of the session: profile generation

Basic Entities

Event: operation performed at specific time

Sequence: set of events, which form states of the sequence

Object: belonging to a resource at a level of abstraction

Operation: gen. action performed on an object

User: accesses resources with ID and Pwd

Resource: Its services are used when a job is being performed

Action: basic operation. Accessors (ReadByte) or modifiers (WriteByte)
