Data Fusion for Improved Situational Understanding

Ambareen Siraj
Department of Computer Science
Tennessee Tech University
asiraj@tntech.edu

Intrusion Detection Systems (IDS) as Sensors for Network Monitoring

- IDSs detect inappropriate or anomalous activity
- Goals
  - Detect wide variety of intrusions
  - Detect intrusions in timely fashion
  - Present analysis in understandable format
  - Be accurate
    - Minimize false positives, false negatives
Multi-Sensor Environment

- No “perfect”/“one-for-all” sensor
- Vary by data source, type of detection, implementation, technique used
- Suite of different sensors can corroborate/complement/challenge each other’s findings

Problem

- Sensors overload security administrators with unmanageable volume of data
- Sensors can be very noisy
- Sensors typically do not add any context or significance to data
- Sensors report only on isolated events
- Sensors cannot shed light on global view
Situation Assessment

- Transformation of low level sensor data to human intelligence
  - To support decision making
  - To aid in taking action

Data Fusion for Situation Assessment

- The process of analysis, interpretation, and combination of alerts to derive a quantitative value such that the value is representative of the extent of concern in the system.
  - Overall condensed security view
**Possibilistic Approach in Data Fusion**

- Based on possibility theory [Zadeh1978]
- Takes uncertainty into consideration
- New application

---

**Unified Fusion Model**

- **Alert Prioritization**
  - Association Assessment
    - **Cluster Generation**
    - **Correlation Link Generation**
    - **Incident Association Assessment**
    - **Situation Assessment**

---

Tennessee Tech University
Multi-Level Alert Clustering

Clustering of two alerts $A_1$ and $A_2$

- Alerts are clustered such that different degrees of deviations in commonality of features are tolerated.

Sadmind Ping

MS SQL Ping

130.080.112.103
130.080.112.102

Multi-level Clustering Assessment

- Derives quantitative value for
  - Clusters activated for host
    - High value
      - Indicates aggregation of multiple alerts with same (highly similar) attributes
    - Low value
      - Indicates aggregation of multiple alerts with less similar attributes
  - Host’s involvement in same/similar attack patterns
    - High value
      - Indicates presence of most specific cluster(s)
    - Low value
      - Indicates presence of less specific cluster(s)
Abstract Incident Model

Abstract Incident Modeling Assessment

- Derives quantitative value for
  - Incidents activated for host
    - **High value**
      - Indicates presence of both evidence and risk
    - **Low value**
      - Indicates absence of either evidence or risk
  - Host’s involvement in multi-staged attack scenarios
    - **High value**
      - Occurrence of one or more highly critical incidents in the correlation chain
    - **Low value**
      - Occurrence of one or more less critical incidents in the correlation chain
Situation Assessment

- Determines overall degree of concern

**Severity**
- Severe
- High
- Significant
- Moderate
- Low

**Cluster Association Strength (CAS)**

**Incidence Association Strength (IAS)**

**Overall Degree of Concern (ODOC)**

Dynamic Fusion

- **Properties**
  - Dynamic
    - Behavior changes
  - Depends on context as well as inputs

\[ \Pi_o(\omega) = \Pi_{i1}(\omega) \otimes \Pi_c(\omega) \]
Dynamic Fusion Approach

- **Context is agreement between inputs**
  \[ h(\Pi, \Pi) = \sup_{\omega \in \Omega} (\min(\Pi(\omega), \Pi(\omega))) \]

- **Behavior changes with context**

Dynamic Fusion Rule

- **Both behavior restricted by agreement**
  \[ \text{Constrained}_\text{HS}(\Pi(\omega), \Pi(\omega)) = \min(\text{HSN}(\Pi(\omega), \Pi(\omega)), h(\Pi(\omega), \Pi(\omega))) \]
  \[ \text{Constrained}_\text{MN}(\Pi(\omega), \Pi(\omega)) = \max(\text{MN}(\Pi(\omega), \Pi(\omega)), h(\Pi(\omega), \Pi(\omega))) \]
Experiments

- **Attack data**
  - MIT Lincoln's Lab's 2000 DARPA Intrusion Detection Evaluation (IDEVAL)
    - Scenario Specific Data Sets

- **Multiple sensor report with different security policy**
  1. RealSecure
  2. Snort

Situation Assessment Results for Multi-Sensor Report
Dynamic Fusion
Results for Multi-Sensor Report

Work in Progress

- **Heterogeneous fusion**
  - Different types of IDS
  - IDS and vulnerability scanners
  - IDS and performance monitoring tools

- **Dynamic fusion**
  - Other factors
    - Reliability
    - Group consensus
  - Asymmetric sources
  - Other applications

Host: 172.016.115.020
IAS= 80.86%
CAS= 79.0%
ODOC= 83.26%

Host: 172.016.113.148
IAS= 0
CAS= 80.86%
ODOC= 45.78%