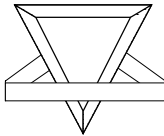


Analysis of the B-SEADS Environment

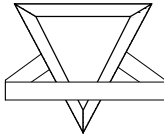
Tysen Leckie



Main Focus

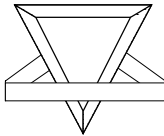
▼ Anomaly Detection

- Strategy of declaring everything that is unusual for the subject suspect, and worthy of further investigation. One of the main issues is to determine what a subject's normal behavior is.
- Uses a statistical method that raises alerts when suspected anomalies deviate from normal behavior.
- Designed to detect novel attacks on the intrusion detection system.
- Possibility of attacker teaching the system that his illegitimate activities are nothing out of the ordinary.
- Usually a high false alarm rate.



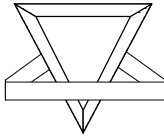
IDS Questions

1. What degree does the IDS detect intrusions into the target system?
2. What is the run time efficiency?
3. Can it detect in real time?
4. How many resources are consumed?
5. How is the ease of use for novice users?
6. Can new intrusion scenarios be added into the system?
7. How resilient is the IDS to attacks on itself?
8. How well does the IDS interoperate with other IDS systems?



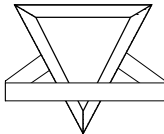
Issues

- Unit of Analysis Problem
 - How much data does the IDS need to examine before it can detect the intrusion, or before it can be said to have missed the detection of an intrusion?
- Detection/False Alarm Rate Trade-Off
 - By classifying more and more events as intrusive (relaxing our requirements on what constitutes an intrusion) we will increase our detection rate, but also misclassify more of the benign activity, and hence increase our false alarm rate.
- Desired Goal
 - Detect a large percentage of intrusions, while keeping the false alarm rate at an acceptable level.



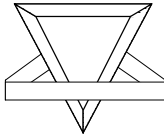
Issues

- Time Granularities – Activity usually has strong time patterns.
- Behavior during different time periods may be different (time of day, weekday, weekend, holiday).
- Time factors should be used in the profiling process to describe a user's normal behavior.



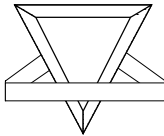
Issues

- ADAM System – Audit Data Analysis and Modeling
 - Developed by Barbara, Couto, Jajodia, Popyack and Wu at George Mason University.
 - Uses data mining to build a customizable profile of rules of normal behavior.
 - A Classifier sifts through the suspicious activities. Marks them as real attacks or false alarms.
 - Designed to be used on-line in real time.
 - Incremental mining algorithms use a sliding window of time to find suspicious events.



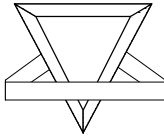
Issues

- **ADAM System**
 - Mines data that is known to be free of attacks to build a repository of normal frequent itemsets that occur during attack free periods.
 - Runs a sliding window algorithm that compares current itemsets with those stored in the normal itemset repository, discarding those deemed normal.
 - Classifier then used to classify the suspicious connections as known attack type, unknown, or false alarm.
 - Itemsets in normal profile database can be categorized by the time of day, day of week, etc.



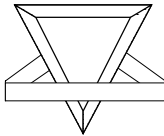
Issues

- **Two Phases**
 - **Phase One – Training Phase**
 - Use data stream where we know where attacks are located.
 - Attack-free parts are fed into module. Output of module is a profile of rules called “normal”.
 - Normal Profile = Behavior during periods of no attacks.
 - Profile + Training Data Set are fed into a module that outputs frequent itemsets that characterize attacks on the system.



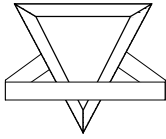
Issues

- Two Phases
 - Phase Two – Intrusion Detection
 - Dynamic algorithm produces suspicious itemsets.
 - These are fed to the Classifier.
 - Classifier labels alarms as attacks (type), unknown or false alarms.
 - Filters false alarms out of itemset. Avoids passing them to security officer.
 - Unknown and Known attacks are given to the security officer.



Bayes

- ✓ Bayesian Detection Rates
 - Base-Rate Fallacy Phenomenon - In order to achieve substantial values of the Bayesian detection rate $P(\text{Intrusion}/\text{Alarm})$, we have to achieve a (perhaps in some cases unattainably) low false alarm rate.
 - The factor limiting the performance of intrusion detection systems is not the ability to identify behavior correctly as intrusive, but rather the systems ability to suppress false alarms.



Issues

- ROC (Receiver Operating Characteristic) Curve Analysis
 - Used to plot the detection rate as a function of the false alarm rate.