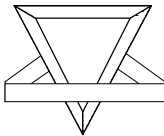
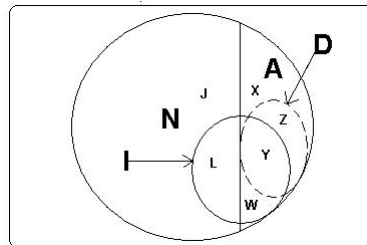


B-SEADS

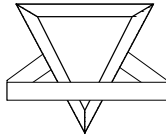
Tysen Leckie



Venn Diagram of Behavior

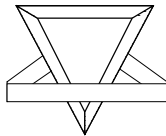


Classification	Intrusion	Event
N = Normal	I = All Intrusions	J = Normal
A = Abnormal	D = Detected Intrusions	L = Undetectable
		X = True Negative
		W = False Negative
		Y = True Positive
		Z = False Positive



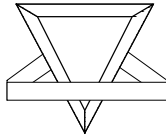
Terms

- Detections – Can only detect intrusions that display abnormal behavior.
- Must define normality or abnormality. Can then distinguish between them.
- Events
 - **Normal (J)** - Ignored.
 - **Undetectable (L)** - Intrusions which display a normal behavior.
 - **True Negative (X)** – Activities which were correctly found to represent no intrusion.
 - **False Negative (W)** – Missed intrusions.
 - **True Positive (Y)** – Correctly detected intrusions.
 - **False Positive (Z)** – Anomalous activities incorrectly flagged as being intrusions.



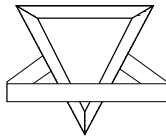
Normal Profile Creation

- Purpose
 - Predict future events by knowing past behavior.
- Only normal behavior is stored.
- Suspicious Behavior - Characterized by deviation from the profile.
- Creation
 - Mine data that occurs during attack-free periods to build the normal profile.
 - Normal behavior should be “clean”. Meaning purely normal and not containing any attacks.
 - Statistical Techniques – Clean normal profile by removing outliers. Negative – time and resource intensive.
 - Better Profile = Less False Positives and False Negatives.



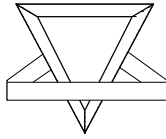
Time Considerations

- Normal behavior different per time intervals.
- Variations help diagnose attacks.
- Able to map each event to a time (timestamp, clock, etc.)



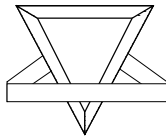
Time Considerations

- **Partition the Normal Profile Database**
 - Weekday Behavior - early morning, morning, afternoon, night, late night.
 - Weekend Behavior - early morning, morning, afternoon, night, late night.
 - Holiday Behavior - early morning, morning, afternoon, night, late night.
 - Early Morning = 12:00 A.M. – 5:59 A.M.
 - Morning = 6:00 A.M. – 11:59 A.M.
 - Afternoon = 12:00 P.M. – 4:59 P.M.
 - Night = 5:00 P.M. – 9:59 P.M.
 - Late Night = 10:00 P.M. – 11:59 P.M.



Metrics Per Time Period

- Number of Initiated Sessions
- Number of Initiated Sessions by Others
- Number of Unique Session Partners
- Number of Repeat Session Partners
- Number of Failed Sessions
- Number of Failed Connection Requests
- Number of Concurrent Sessions with at Least one Shared Partner
- Number of Failed Requests of Trusted Third Parties



Attack Detection

- Statistical Anomaly Detection Models
 - Operational Model - Based on thresholds. An event reaches a certain threshold (number).
 - Mean and Standard Deviation Model - Raises an alarm if an observation does not lie within a given confidence interval.
 - Time Series Model - Takes the time at which an event takes place into account. If probability for that event at that particular time is too low an alarm is raised.
 - Bayes Estimators – Detects unknown attacks.
- Possible Results:
 - Suspicious:
 - Low
 - High
 - Attack