

Next-Generation Intrusion Detection Expert System(NIDES)



Debra Anderson, Teresa Lunt
Harold Javitz, Ann Tamaru, and
Alfonso Valdes
May 1995

What is NIDES?



- Intrusion detection system that performs real-time monitoring of user activity
- Performs 2 types of analysis(statistical and rule-based)
- Statistical analysis- maintains historical profile of a user and raises an alarm when observed behavior differs from established patterns of use



Half-Life

- Determines the number of audit records or days of audit record activity that constitute short-term and long-term behavior
- Ex. Set half-life = 30 days
 - Records gathered 30 days ago contribute half as much weight toward the probability distribution as most recent records
 - Records 60 days ago contribute $\frac{1}{4}$ and so on
- Aging rate- existing information in a profile is aged, the smaller the rate, the more rapidly this information is forgotten



NIDES measures

- Activity intensity
 - Measures the rate at which activity is progressing
 - Used to detect abnormalities in bursts of behavior that may not be detected over longer term averages
 - Ex. Number of audit records processed for a user in 1 minute



NIDES measures(cont.)

- Audit record distribution
 - Measures the distribution of all activity types in recent (like the last few hundred) audit records
 - Ex. Relative distribution of file accesses and I/O activity over the entire system usage for a particular user



NIDES measures(cont.)

- Categorical
 - Measure the distribution of a particular activity over categories
 - Ex. Relative frequency of logins from each physical location, the relative usage of each compiler, shell, editor, etc. in the system



NIDES measures(cont.)

- Continuous
 - Measures activity whose outcome is a numeric value
 - Ex. The amount of CPU and I/O used by a particular user
 - Statistics are computed on the numerical value of the activity outcome



Statistical Approaches

- Q Statistic – the degree of difference between a long-term profile and short term profile measure
- S and T^2 Statistic
- Bayesian Statistics
- Belief Networks
- Predictive Pattern Generation
- Neural Networks



References

- "Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System(NIDES)", Anderson, Lunt, Javitz, Tamaru, Valdes, May 1995
- "Classification and Detection of Computer Intrusions", Kumar, Purdue University, August 1995