Network Intrusion Detection and Alert Correlation

Xiaosong Lou and Ying Chen, {xlou, chen2}@usc.edu

Stop Intrusion Before It Completes

Problem
- Number of intrusion alerts overwhelms the system administrator
- Attack Scheme usually takes multiple steps
- Blocking traffic from source IP would lead to disruption of service because of false positive

Solution
- Reducing the amount of alerts sent to system administrator
- Making predictions for the next step in the attack scheme

Collaborative Intrusion Detection with Rule-Based Signature Generation

- Combine misuse-based IDS with Anomaly Detection System to detect both attacks with and without signatures
- Datamining of Internet connection episodes for normal traffic profiling and automated attack signature generation

Related Publications:

Alert Clustering and Prediction for Intrusion Prevention

- Based on the inherent temporal relations among intrusion alerts
- Number of alerts is reduced for more than 90%
- Most attack patterns are disrupted with low mis-prediction rates
- Performance insensitive to parameter variations lead to easier implementation

Related Publication:

Performance Evaluation of CAIDS

- The experiment is based on DARPA 1999 Intrusion Detection Evaluation Data Set mixed with real network data from USC
- On the average, the CIDAS outperforms Snort and ADS by 51% and 40% improvement in intrusion detection rate, respectively

ROC curves for four attack classes in using the CIDAS

ROC curves showing the average intrusion detection rates of 3 systems