Information Visualization for an Intrusion Detection System

J. Blustein, C.-L. Fu, & D. L. Silver

Objective: A user interface supporting network information visualization for an Intrusion Detection System (IDS).

1. Help the users to filter/recognize the most important messages from many messages generated by IDS
2. Flexible and adaptable to the users
3. Assists users in overcoming false detections from IDS

Problems

Current IDS have several problems that frustrate optimal security efforts:

1. **Too many false detections**
   a. High traffic volume reduces effectiveness of even the best IDS
   b. Assuming 0.01% false alarm rate x 100,000 events per day = 10 false alarms every day (Both false negative & false positive)
   c. Current typical false alarms for a good IDS: about 5%

2. **IDS detections do not get immediate attention -** high volume of detections (including many false ones) make immediate response difficult.

+

Spatial Hypermedia

Information Triage – sorting through numerous relevant materials and organize them to meet the needs of the tasks at hand.

1. Suitable for information intensive tasks
2. New patterns can be recognized from the objects on the workspace as the user is working to find a solution.
3. Visually oriented workspace allows the user to recognize familiar patterns and respond immediately.
4. Patterns that are difficult to put into words can be presented to the user with simple spatial cues (color, proximity, alignment, orientation, etc.), and the presentation may be recognized immediately.
5. Containment - able to present the big picture, yet the user can reveal the details very quickly.

=

Proposed Solution

1. Allow users to visualize network in many dimensions
   a Time, flow, event types, etc.
2. Users can recognize developing patterns
   a Gain a sense of normal network activities
   b Recognize intrusion *as it happens*, not after
3. ***Translation Module*** makes it possible to adopt the user interface to many different IDS programs
4. ***Recommendation Agent*** gives suggestions unobtrusively to assist the user to sort the objects on workspace – so that the user can recognize anomalies more easily.
5. ***User Modelling Agent*** – develops a user model that allows the system interface presentation to be adapted to the user.