Information Security Storm Map

Technology is rapidly changing. Due to the changes, there are new access points to information and new applications for information exchange and exploitation. These changes increase the complexity of monitoring and analyzing potential system and information compromises. For example, devices such as Apple's iPhone/iPod, netbooks, mobile wireless access points, etc. have changed how and where we connect to the Internet. Therefore, the perimeters of company, school, and home networks have been extended to the point of almost blurred.

When a compromise occurs, there is a large volume of monitoring data. Granted, there are tools that are able to analyze this data from a specific domain (i.e. switch, server, firewall, etc.). However, an intuitive holistic view/analysis has been lacking. Therefore, we are proposing a visualization that provides a weather map type view of security events occurring on a network.

How will a weather map view provide a holistic view of security events? First each component of the network will be added as a node in a network diagram with the ability for data abstraction and drill down. This provides the capability to show relationships between each node (i.e. which server or PC is connected to which switch, where the devices are physically located, etc.). Building on this metadata allows for additional meaning to be added when an event occurs because a user of the visualization can see where events are occurring, the severity of the event, and which nodes can potentially be affected.

What features will the visualization provide? There will be two views of the data provided: 1) the weather map view and 2) the network layout view. The weather map view will start with a set of physical locations and how each are linked together. From each location the user will be able to drill down and view the devices/nodes that are in that location. At the switch/abstracted level the user will be able to see icons for the types of events that are occurring on the devices connect to that switch. This provides a similarity between our security weather/storm map and a meteorological weather map. In a meteorological weather map like Doppler radar icons in reference to high and low fronts, hurricanes and snow storms are visible and intuitive. Therefore, we would like to take a similar approach with security storms. The collection of icons will be used as a legend to describe the types of security storms. The user will be able to select nodes in order to obtain additional information such as detailed description of the events and severity that are occurring via a popup window. From the network layout view, the user is able to see the devices connected to each switch at each physical location what type of security events are occurring. The users will be provided a preferences panel. The components provided on the panel will allow a user to customize their view so that they can see the information relevant for their needs. They will be allowed to turn off and on the icons for various types of events from the view layout.