Visualizations to Improve Reactivity Towards Security Incidents Inside Corporate Networks

Patrick Hertzog
User Experience Officer, NEXThink S.A.
January 12th, 2007
About NEXThink

- Founded in September 2004
- Headquartered in Lausanne, Switzerland
- Develops and commercializes REFLEX™, a solution for Insider Threats Management based on research initially conducted at the AI Lab of the Swiss Federal Institute of Technology (EPFL)
Reactivity towards security incidents

Why is reactivity important?
- Minimize impact on business
- Legal responsibility
  - Attacked network can become the source of another attack
  - Corporations have to take measures to report such incidents to authorities within an acceptable time period

Security administrators are flooded by non-pertinent information
Our approach

- Visualization-based tools can help administrators to take quicker and better decisions

However, we are facing two major challenges:
  - Lack of pertinent information
  - Amount of data to display
Lack of pertinent information

- Most current systems are based on a high number of low-level parameters
  - Decision process lengthened
  - Incertitude introduced

- We focus on a small set of certain high-level parameters for each connection
  - Time
  - User (e.g., Windows SID)
  - Application (e.g., firefox.exe)
  - Source host
  - Destination port and host
Amount of data to display

- Even when focusing only on pertinent data, we still have a lot of information to display.

- Displaying that information with a fine granularity is clearly not feasible.

- We introduce an interactive grouping technique for visualizations:
  - Group similar information
  - Possible to drill down to get more precise information
Grouping technique

- Each node has a state attribute
  - collapsed = displayed as a group
  - expanded = children displayed individually

Organization of the network items in a tree structure

Computation of an optimal tree state

Mapping of the tree state to the graphical representation

User-triggered grouping / ungrouping

Internet tools

- browsers
  - firefox.exe
  - iexplore.exe
  - opera.exe

- email clients
  - thunderbird.exe
  - outlook.exe

© 2007, NEXThink S.A. - Public Information
Grouping technique (2)

- Computing a tree state means setting the *state* attribute of each node.
- It has to respect some constraints.

- Screen real estate is limited and each network item (or group) needs a minimal amount of space.
- The maximum number of network items (or groups) should be displayed.
- The user actions (manual grouping / ungrouping) have to be respected.
To take the right decision, security administrators need first to understand generated alarms

- Rule-based systems: alarms easy to understand
- Anomaly-based systems: alarms difficult to understand

Our claim: To understand what is abnormal, one needs first to understand what is normal

We want to display normal connections along with alarms
Visualizing connections (2)

- Connections can be seen as tuples \(<\text{time, user, application, source host, destination port, destination host}>\)

- A parallel-coordinates visualization is a good idea to display such information

- However, there are challenges related to the number of lines to be drawn
  - It becomes quickly unreadable and therefore unusable
  - It is prone to deception attacks
Our grouping technique and the abstraction of time reduce dramatically the number of lines.

More than 17 millions connections displayed in a parallel-coordinates visualization.
Visualizing connections – Interaction
Visualizing connections – Interaction (2)

The mouse cursor is moved over office applications and corresponding connections are highlighted.
Visualizing connections – Interaction (3)

Office applications are ungrouped to provide a more detailed view
Usage scenario I – Why was this alarm generated?

- One can clearly see that this application usually makes connections through another port.
Usage scenario II – Who is using port 22?

- The port 22 is often open for SSH communication but who is using it, with which applications and to connect to which computer?

- If one wants to close that port, who will be affected?
Visualizing activity and alarms over time

- Parallel-coordinates visualizations are useful to help understand single alarms but not to see correlations between alarms

- We use a visualization based on a scatterplot to display activity and alarms over time
  - X-axis represents the time
  - Y-axis represents a type of network items (i.e., either users, applications, sources, ports or destinations)

- Our grouping technique helps to limit the number of rows
Visualizing activity and alarms over time (2)

- Brighter blue indicates more activity
- Colored rectangles represent alarms
- The visualization is augmented by two histograms representing the sum of alarms by time (on the top) and by network item (on the right)
An example
A new approach to build visualizations based on pertinent information and a grouping technique has been presented.

Presented visualizations are part of REFLEX™ commercialized by NEXThink.
Thank you for your attention!!

Patrick Hertzog
patrick.hertzog@nexthink.com
http://www.nexthink.com