NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows

Ratna Bearavolu, Kiran Lakkaraju, William Yurcik
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign
Outline

• Motivation
• Situational Awareness & Visualization
• Visualization Criteria
• NVisionIP – Demo
• Conclusion
Motivation

• Motivated by the concerns of Security Engineers at NCSA
• How do you provide situational awareness of the network – awareness of the state of the devices on the network
• Focus on situational awareness then intrusion detection
• Wanted a tool where the user can see the state information of the devices on the network
Situational Awareness Using Visualization

• Use visualization to show information about the network

• Visualization is used because it is:
  – Easy to detect patterns in the traffic
  – Conveys a large amount of information concisely
  – Can be quickly created by machines

• Use the security engineers background knowledge and analysis capabilities along with the capability of machines to quickly process and display data.
Key Features of Network Visualizations for Security

- **Interactivity:** User must be able to interact with the visualization
- **Drill-Down capability:** User must be able to gain more information if needed
- **Conciseness:** Must show the state of the entire network in a concise manner
Interactivity

• Allow security engineer to decide what to see
  – Data views (Cumulative, Animation (interval lapse) and Difference)
  – Features to view (traffic in/out, number of ports used, etc)
  – Filtering
Drill-down capability

- Allow security engineer to see the network at different levels of resolutions
- Entire network – Galaxy View
- A subset of hosts – Small Multiple View
- A single machine (IP) – Machine View
Conciseness

• Allow a security engineer to view a large amount of information concisely
  – Show entire network with minimum of scrolling

…..thus allow security engineer to gain situational awareness of the network
Where is the data coming from at NCSA?
For a single IP

- **FlowCount** - Number of times IP address was part of flow (Flow Count)
- **SrcFlowCount, DstFlowCount** – Number of time IP address was source and destination of a flow
- **PortCount** – Number of unique ports used
- **SrcPortCount, DstPortCount** – Number of unique ports used as source and destination ports
- **ProtocolCount** – Number of unique protocols used
- **ByteCount** – Number of bytes transferred.
Getting NVisionIP

- Distribution Website:
  http://security.ncsa.uiuc.edu/distribution/NVisionIPDownLoad.html

- SIFT Group Website:
  http://www.ncassr.org/projects/sift/
Conclusion

• Combine Security Engineers’ skills with the visualization capabilities of machines.

• Visualizations with three key properties to provide Situational Awareness:
  – Interactivity
  – Drill-Down Capability
  – Conciseness
Questions