Tool Update: *NVisionIP* Improvements (Difference View, Sparklines, and Shapes)

William Yurcik
National Center for Supercomputing Applications (NCSA)
University of Illinois at Urbana-Champaign (UIUC), USA
byurcik@ncsa.uiuc.edu

ABSTRACT
This paper highlights major enhancements made to the security visualization tool – *NVisionIP* – since it was first presented at the VizSEC/DMSEC 2004 Workshop.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *security and protection;* C.2.3 [**Computer-Communication Networks**]: Network Operations – *network monitoring;* H.5.2 [**Information Interfaces and Presentation**]: User Interfaces – *graphical user interfaces (GUI);* I.3.6 [**Computer Graphics**]: Methodology and Techniques – *interaction techniques;* K.6.5 [**Management of Computing and Information Systems**]: Security and Protection.

General Terms
Security, Human Factors

Keywords
security visualization, IP address space visualization, traffic visualization, sparklines, difference view, NetFlows

1. INTRODUCTION
This short paper highlights enhancements to *NVisionIP* since it was made available for Internet download [3] and presented at VizSEC/DMSEC'04 [5]. *NVisionIP* is the only tool to have been presented at each of the VizSEC workshops 2004-2006 [4,5].

2. BACKGROUND
NVisionIP is a security visualization tool which represents the state of all IP addresses within an IP address space using a multilevel grid interface [2,5,6,7,8]. The state of each IP address is measured in terms of in/out flows and characteristics of these flows (see Table 1). Multiple levels of *NVisionIP* are at the interactive control of the user. Figure 1A shows three levels linked by mouse drill-down. Figure 1B is a Galaxy View (GV) overview of an entire IP address space through use of colored dots on a grid with each color representing a user configurable metric as defined in Table 1. Figure 1C is a Small Multiple View (SMV) which allows a user to quickly scan flow activity of subnets within an address space via the use of colored histograms corresponding to ports/services. Figure 1D is an individual Machine View (MV) with tabs showing all flow activity in/out. The lowest level is not shown – an MV tab displays raw source data (NetFlows in this case). Time is indicated by the selected log file, digital timestamp, and analog clock. GV animation occurs by displaying selected log file segments in quick sequence.

Table 1. *NVisionIP* Metrics per IP Address

FlowCount	number of times IP address was part of flow
SrcFlowCount, DstFlowCount	number of times IP address was source/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

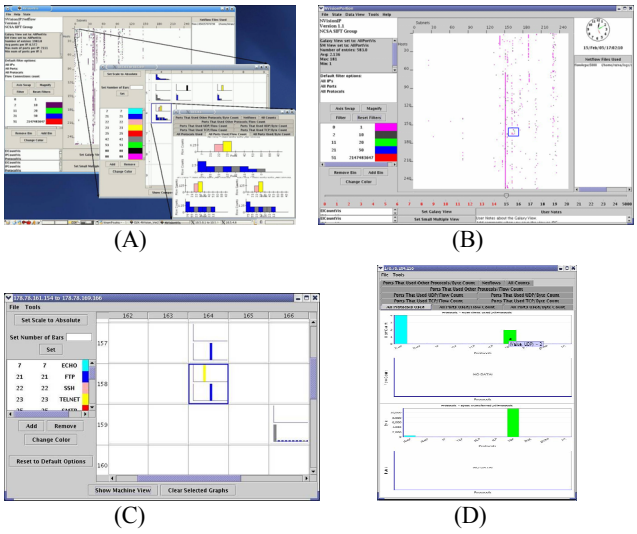


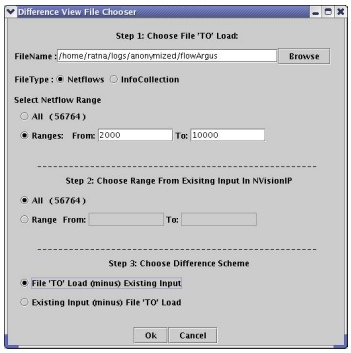
Figure 1. *NVisionIP:* (A) linkage between 3 levels; (B) Galaxy View; (C) Small Multiple View; and (D) Machine View.

VizSEC'06, November 3, 2006, Alexandria, Virginia, USA.
ACM 1-59593-549-5/06/011.

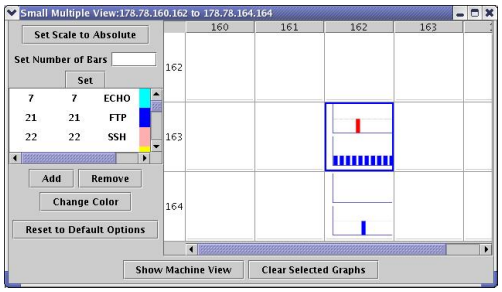
3. ENHANCEMENTS

There have been several enhancements to *NVisionIP* including optimal redesign of source code for performance (especially for animation) and Closing-the-Loop [1,4]. This paper focuses on the (1) difference view, (2) sparklines, and (3) shape enhancements.

The difference view is a basic but powerful function – it allows a user to compare log files by subtracting one from the other. The function is motivated by a desire to compare traffic under study with benchmark traffic. If benchmark traffic is normal then the difference view will display anomalous traffic. If the benchmark traffic is malicious, the difference view show normal traffic and validate a match with suspected malicious traffic. Figure 2 shows the difference view GUI and an example difference view at the SMV level. While the difference view greatly reduces human analysis processing, obtaining benchmark traffic for particular environments may be difficult.



(A)



(B)

Figure 2. *NVisionIP* Difference View: (A) GUI; (B) Difference View at the SMV Level

Sparklines show context of how displayed values compare to recently past values to help determine if a value is within range or out-of-range as well as recent trends. Sparklines are mouse-over events per IP address in the *NVisionIP* GV. Figure 3 shows a sparkline for a particular IP address, the current count of 7 is significantly higher than recent counts and may indicate an anomalous increasing count trend or malicious activity.

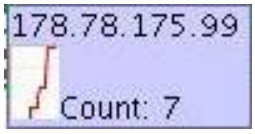


Figure 3. *NVisionIP* Sparkline

Leveraging human visual processing, pixels for IP addresses may be user-selected to form shapes other than dots. Figure 4 shows IP addresses as lines oriented in different directions. Triangles and boxes are other shapes. Humans more easily discriminate shapes at different orientations than colors so shapes may be used to enhance detection of different metrics (along with magnification).

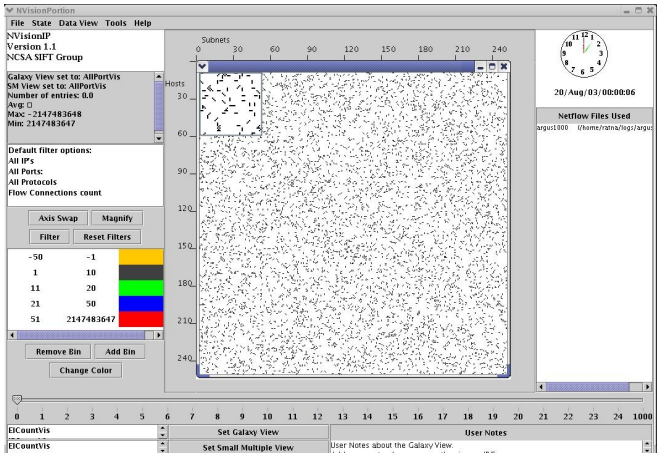


Figure 4. *NVisionIP* GV with Line Shapes (magnification in upper left corner)

4. ACKNOWLEDGMENTS

Kiran Lakkaraju was the initial software developer of *NVisionIP* and the enhancements in this paper were implemented by software engineer Ratna Bearavolu, both under supervision of the author.

5. REFERENCES

[1] Bearavolu, R., Lakkaraju, K., and Yurcik, W., *NVisionIP*: An Animated State Analysis Tool for Visualizing NetFlows, *FLOCON – Flow Analysis Workshop*, 2005.

[2] Bearavolu, R., et al. A Visualization Tool for Situational Awareness of Tactical and Strategic Security Events on Large and Complex Computer Networks, *IEEE Military Comm. Conf. (Milcom),* 2003.

[3] *NVisionIP* Download Page <http://security.ncsa.uiuc.edu/distribution/NVisionIPDownLoad.html>

[4] Lakkaraju, K., et al. "Closing-the-Loop in *NVisionIP*: Integrating Discovery and Search in Security Visualization," *2nd Intl. Wkshp. on Vis. for Comp. Security (VizSEC),* 2005.

[5] Lakkaraju, K., et al. *NVisionIP*: NetFlow Visualizations of System State for Security Situational Awareness, *Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC),* 2004.

[6] Lakkarju, K. et al. *NVisionIP*: An Interactive Network Flow Visualization Tool for Security, *IEEE Intl. Conf. on Systems, Man, and Cybernetics (SMC),* 2004.

[7] Lakkaraju, K. *NVisionIP* – A Traffic Visualization Tool for Security Analysis of Large and Complex Networks, *Intl. Multiconference on Measurement, Modelling, & Evaluation of Comp.-Comm. Systems (Performance TOOLS),* 2003.

[8] Yurcik, W., et al. A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection, *Workshop on Data Mining for Computer Security (DMSEC),* 2003.