Tool Update: *VisFlowConnect-IP* with Advanced Filtering from Usability Testing

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 – *VisFlowConnect-IP* – 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
Experimentation, Security, Human Factors,

Keywords
security visualization, parallel coordinates, traffic visualization, anomaly detection, intrusion detection

1. INTRODUCTION
VisFlowConnect-IP was first presented at the VizSEC/DMSEC Workshop in 2004 [5] and since then has evolved with feedback from usage in numerous production environments and formal usability experimentation [1]. This short paper highlights the major enhancements to *VisFlowConnect-IP* since 2004.

2. BACKGROUND
As first presented in 2004, *VisFlowConnect-IP* is a link analysis tool which represents IP traffic flows in parallel coordinate views that dynamically change in time under user control [5,6]. Figures 1 and 2 present the three parallel coordinate views which are described in more detail in [5,6]. The focus in 2004 was to provide a transparent view of all network traffic to security engineers so they could monitor in real-time or play-back in retrospect. Our design emphasized scalability (no state information saved over time) so the tool could be run for long periods of time (days, months)

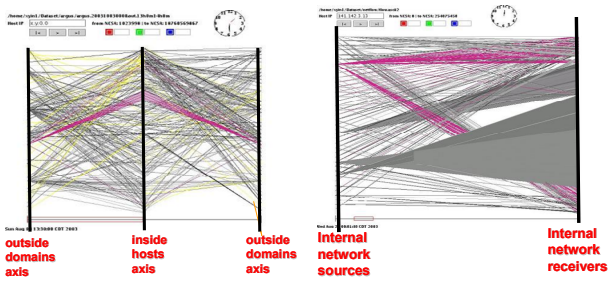

Figure 1. *VisFlowConnect-IP* Main and Internal Views [5,6]

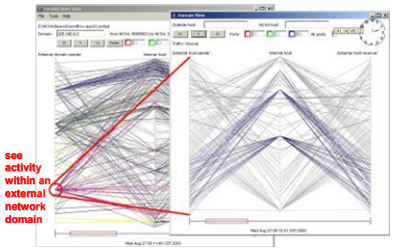

Figure 2. *VisFlowConnect-IP* Domain View [5,6]

Since *VisFlowConnect-IP* has been made freely available on the Internet [2], it has been downloaded thousands of times and we have received feedback on its use in production environments which we now summarize.

The most frequent feedback was the format of the NetFlows source data input to *VisFlowConnect-IP* so we independently developed a tool to convert NetFlows between formats. The ability to stop/start *VisFlowConnect-IP* and to view ports information on traffic links – while both of these are desirable but implementation would affect scalability. Next the ability to filter traffic for two reasons: (1) so "good" traffic could be deleted and "traffic of interest" could be better examined without being obscured and (2) the ability to highlight traffic of interest in contrast to other traffic – similar to signature alarms from intrusion detection systems.

3. ENHANCEMENTS
VisFlowConnect-IP is designed to read from NetFlow log files of any size with a buffer to read in a finite amount of records (as

VizSEC'06, November 3, 2006, Alexandria, Virginia, USA.
ACM 1-59593-549-5/06/0011.

shown in Figure 3), reorder them, and then send them to the visualization engine. Scalability in terms of the log file size is only relative to this buffer insertion of new records. The next scalability factor is the time window size configurable by the user – as traffic within a time window increases, processing delay also increases. We report performance results for scalability in terms of log size and window size in [4].

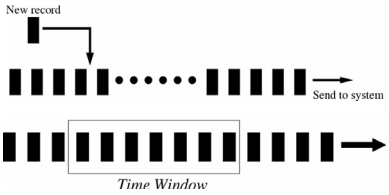

Figure 3. Scalability: Time Window Algorithms [4]

IP address space scalability is challenge. *VisFlowConnect-IP* was designed for a class B IPv4 address space so use on class B or Class C address spaces is not a problem. Several engineers have used *VisFlowConnect-IP* on networks consisting of multiple class B address spaces by using multiple *VisFlowConnect-IP* instances/windows. In monitoring one class B address space, if more IP addresses are active than can be accommodated then we have implemented an IP-shedding algorithm documented in [4].[1] If the traffic intensity and corresponding window size is such that many IP addresses appear and drop-out of the time window maintaining a stable GUI location for a particular IP address is difficult. Since we sequentially order IP addresses, vertical movement of IP addresses up-and-down can be misinterpreted. To mitigate this effect we implement algorithms to move in only one direction so an IP address may slowly drift as shown in Figure 4 as opposed to jitter up-and-down.

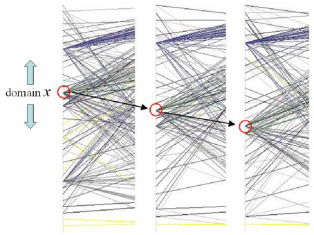

Figure 4. Scalability: IP Address Space Dynamics [4,7]

Filtering was initially implemented in 2004 with highlighted port boxes as show in Figure 6 [5,6] but later enhanced with a system dialog box [4] and further enhanced with a filtering language [3,7] as shown in Figure 7. While traffic links were distinguishable via intensity (black thickness) and targeted ports by colors (red,green,blue), the amount of traffic often obscured these effects. The dialog box has evolved to select different protocols, traffic intensities, packet sizes, and excluded ports with the traffic loaded into the *VisFlowConnect-IP* system. The language implemented allows traffic to be filtered before being processed into the *VisFlowConnect-IP* system and thus improves both scalability (performance) and analysis ability.

[1] Another option considered was lengthening the vertical axes along with scrolling but dynamically changing GUI size was rejected in user tests.

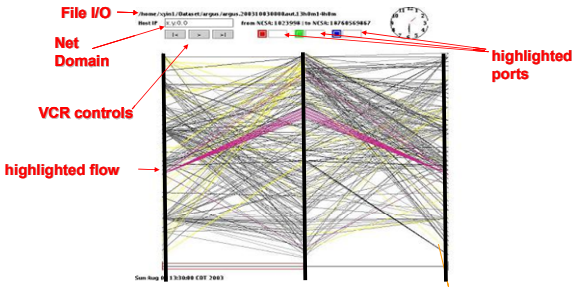

Figure 6. *VisFlowConnect-IP* Filtering Controls [5,6]

```
+:(SrcIP=141.142.0.0−141.142.255.255),
+: (SrcPort=1−1000)
//keep all records from domain 141.142.x.x,
// from port 1 – 1000
−: (SrcPort=80)
−: (DstPort=80)
//discard records of http traffic
```

Figure 7. *VisFlowConnect-IP* Filtering Language [4,7]

4. ACKNOWLEDGMENTS

Xiaoxin Yin is the *VisFlowConnect-IP* software developer (2003-2006) under supervision of this author. Usability experiments were performed by Ramona Su Thompson under supervision of the author and Esa M. Rantanen (UIUC).

5. REFERENCES

[1] Thompson, R.S., Rantanen, E.M., and Yurcik, W., Network Intrusion Detection Cognitive Task Analysis: Textual and Visual Tool Usage and Recommendations, *50th Meeting of the Human Factors and Ergonomics Society (HFES),* 2006.

[2] *VisFlowConnect-IP* Download Page <http://security.ncsa.uiuc.edu/distribution/VisFlowConnectDownLoad.html>

[3] Yin, X., Yurcik, W., and Slagell, A., VisFlowConnect-IP An Animated Link Analysis Tool for Visualizing NetFlows, *FLOCON – Flow Analysis Workshop*, 2006.

[4] Yin, X., Yurcik, W., and Slagell, A., The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness, *3rd IEEE Intl. Workshop on Information Assurance (IWIA)*, 2005.

[5] Yin, X., Yurcik, W., Treaster M., Li, Y, and Lakkaraju, K., VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness, *Workshop on Visualization and Data Mining for Computer Security (VizSEC/DMSEC),* 2004.

[6] Yin, X., Yurcik, W., Li, Y, Lakkaraju, K. and Abad, C., VisFlowConnect: Providing Security Situational Awareness by Visualizing Network Traffic Flows, *IEEE Intl. Perf. Computing & Comm, Conf. (IPCCC),* 2004.

[7] Yurcik, W., VisFlowConnect-IP: A Link-Based Visualization of NetFlows for Security Monitoring, *FIRST Conf. on Computer Security Incident Handling*, 2006.