

Applied Security Visualization

Review by JP Bourget, CISSP, MCSE, MS

Having a process to better understand your logs, be it firewall, packet captures, IDS, web server, or proxy logs, is something that many security professionals strive for. We have seen some interesting software over the past few years, such as OSSIM and Splunk. Some vendor's provide excellent log visualization for their products, some don't do enough, or aren't flexible enough. That brings along Applied Security Visualization (ASV) by Raffael Marty. Marty's book gives some valuable insight on how to bridge the fields of IT Security and Data Visualization all in one book. While this book provides a wealth of detailed knowledge, I'm going to point out the major features instead of getting really detailed.

Free Chapter Link Below

Chapter 5 - Visual Security Analysis

[del.icio.us](#)

Discuss in Forums {mos_smf_discuss:Book Reviews}

Free Sample Chapter

Chapter 5 - Visual Security Analysis

This is one of those tech books that is a good read from beginning to end. The book starts out explaining many of the

benefits of visualization. And, unlike many technical books, Chapters 1 – 3 gives us the groundwork to actually start graphing some data right away. The most significant point made by Marty is the time it takes the brain to make a relationship with a visual map of data compared with understanding the same data as text or log files. Marty does a good job of giving us a primer on visualization theory such as the Gestalt Principles, and the different common graph types and their importance. Then Marty proceeds into Chapter 2, explaining the important parts of common data outputs such as tcpdump, Cisco Netflow, Firewall and OS logs, and a few others.

Finally, we finish getting up to speed in Chapter 3, which gives us a detailed understanding of the different types of graphs such as Link Graphs, Parallel Coordinate Graphs, and my favorite – Three-Dimensional Scatter Plots. Now that we have an idea of what visual modes are out there, Marty provides us on p110 – 113 with an excellent “at a glance” table. This shows us what graphs will work well with different situations. It’s tables like these that will make this a good reference book for years to come.

Now that we have a good foundation, Marty shows us his methodology for the Information Visualization Process. The steps are to define the problem, assess the available data, process information, visual transformation, view transformation, interpret and decide. When you get to processing information, we are presented with a list of ideas on how to parse various types of logs, with tools freely available at <http://secviz.org>, and he explains some techniques on how to add data (like DNS host names) when you get IP addresses. You will also learn about some other processing techniques, such as aggregation, filtering, and to be on the lookout for inconsistent log files.

The visual transformation step goes into how we can map our data, referring to the table (mentioned above) that helps us decide what type of graph will work best. You will understand that you really need to experiment with what you want the focus of your graph to be by reading this chapter. Marty also explains the application of shapes, size and color, and points out that color increases legibility beyond size and shape. Finally, after doing any necessary adjustments to our view, the last step is to interpret and decide what happened, and make sure our graph or graphic shows what we intended to show in the first place.

Chapter 5 moves along to Visual Security Analysis. Marty covers reporting, historical analysis and real time monitoring. Most of you have probably seen moving averages and trend graphs, but Marty really gets into the act with correlation graphs (with code to generate a correlation graph) which show the relationship between two events. Then we get into forensic analysis, from inputs such as netflow, to find attacks. Figure 1 shows an example graph of apache logs from the SecViz Graph Exchange. Marty also gets into some AfterGlow configuration. AfterGlow is an open source collection of scripts used to generate graphs. My Favorite technique in this chapter is the CISO dashboard. This dashboard which you can see on page 233 of the sample chapter (link above), shows a red/yellow/green light status along with a cost analysis of the current incidence, as well as compliance and risk status for a network. You can see trends over time to indicate the level of performance of your team and/or network.

Figure 1: Graphing Apache Logs (Source: <http://secviz.org/content/picviz-graphing-apache-logs>)

Chapter 6 continues on the theme for Chapter 5, but takes us to perimeter threats, showing some really interesting examples on doing visual IDS, firewall, snort, and email log correlation. There is a script Marty shows us to extract social network relations out of email logs, as a number of treemaps with regards to vulnerability scanning. Figure 2 shows an example of open ports based on an nmap scan.

Figure 2: Treemap of Open Ports Nmap Scan (Source: <http://secviz.org/content/open-ports-a-bunch-servers>)

Chapter 7 jumps into visualizing compliance, such as database monitoring and separation of duty graphs, while Chapter 8 goes into some methods for detecting insider threats. Pages 434 – 443 provide the reader with a comprehensive set of precursors to insider threats and crimes (a nice bonus for a visualization book).

ASV wraps up with a nice review of many of open source and/or free data visualization tools, many of which are included in the DAVIX LiveCD (included with the book or download [here](#)). The author lists the strengths of these tools, and also a lot of config and command line samples.

ASV is a must have book for any Info Security Analyst who has a need to visualize the information that they deal with. My only complaint is that the author doesn't always show or detail how he generated certain graphs. ASV gives you a good reference and starting point to go out and apply what is in the book, and is accompanied by secviz.org, a portal to share new graphs and parsers, as well as updates to the book. This is not a book you can read through quickly, but a book you can get lost in and come out of your stupor with great insight on the details of visualizing data, which will no doubt help many security professionals not educated in visualization theory.

Jean Paul (JP) Bourget, BS IT, RIT 2005; MS Computer Security and Information Assurance, RIT 2008; CISSP; MCSE, CSSA. JP has five years experience in computer networking, system administration, and information security. During the day JP is responsible for Network and Security Management for a medium size global company based in the US. JP is also adjunct faculty at Rochester Institute of Technology where he teaches Networking and Security undergraduate classes. JP also performs pen testing and security audits for local companies in Rochester, NY. In his spare time, JP snowboards, rides motorcycles, mountain bikes and enjoys fixing up older homes.