Errata

Here are a few typos and errors that I have found or others have found in the book. Thanks for reporting them (either via email to me or as a comment here).

- Inside cover: My name is misspelled (Rafael instead of Raffael)
- Page 15, Figure 1-7: Similarity should be Similarity in the top right of the figure.

Use Visualization to Secure Your Network Against the Toughest, Best-Hidden Threats

As networks become ever more complex, securing them becomes more and more difficult. The solution is visualization. Using today’s state-of-the-art data visualization techniques, you can gain a far deeper understanding of what’s happening on your network right now. You can uncover hidden patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures that are far more likely to succeed than conventional methods.

In Applied Security Visualization, leading network security visualization expert Raffael Marty introduces all the concepts, techniques, and tools you need to use visualization on your network. You’ll learn how to identify and utilize the right data sources, then transform your data into visuals that reveal what you really need to know. Next, Marty shows how to use visualization to perform broad network security analyses, assess specific threats, and even improve business compliance.

He concludes with an introduction to a broad set of visualization tools. The book’s CD also includes DAVIX, a compilation of freely available tools for security visualization.

You’ll learn how to:

- Intimately understand the data sources that are essential for effective visualization
- Choose the most appropriate graphs and techniques for your IT data
- Transform complex data into crystal-clear visual representations
- Iterate your graphs to deliver even better insight for taking action
- Assess threats to your network perimeter, as well as threats imposed by insiders
- Use visualization to manage risks and compliance mandates more successfully
- Visually audit both the technical and organizational aspects of information and network security
- Compare and master today’s most useful tools for security visualization

Contains the live CD Data Analysis and Visualization Linux (DAVIX). DAVIX is a compilation of powerful tools for visualizing networks and assessing their security. DAVIX runs directly from the CD-ROM, without installation.
Press / Related Material

- February 2010, Directed musings on computers, music, huskies, ...
- March 2009, doing more with less … on the SecurityKitchen.
- February 2009, Better security through better visualization by Michael Kelly.
- February 2009, BOOK EXTRACT: Applied security visualization
- December 2008, iLogin Book Reviews
- December 2008, Book review on Windows IT Pro
- November 2008, Book review on Slashdot
- November 2008, Raffy's Visualization Book Blog post by Anton Chuvakin
- September 2008, Book Review by Adam Shostack
- September 2008, Q&A: Security Visualization Interview with Mirko Zorz
- August 2008, Book Review by Francois Ropert
- August 2008, Security visualization helps make log files work Article by Robert Westervelt
- August 2008, Book Extract: Networking data visualisation explained
- August 2008, Interview with Martin McKeay at DefCon 2008 (podcast)
- March 2008 SOURCE Boston Blog about "All the data that's fit to visualize" talk.
- January 2008 Bridging Visualization and Security (video)
- January 2008 Applied Security Visualization (video)
- August 2007 Bar Talk about Security Visualization (podcast)
- May 2007 Applied Security Visualization at First 2007 (podcast)
Past events

- IT GRC Visualization, Triangle InfoSeCon, Raleigh, North Carolina, October 2008.
- IT Security Awareness Event at University of Michigan, October 2008.
- Panel discussion at VizSec, Boston, September 2008
- DAVIX presentation at VizSec, Boston, September 2008
- FIT-IT, Graz, Austria, September 2008
- Workshop on Visualization at DefCon, Las Vegas, August 2008
- "All the Data That's Fit To Visualize", SOURCE Boston, March 2008

In the spirit of sharing and

On March 14th, 2011 adnan202 says:

In the spirit of sharing and in the hopes of prodding a co-conspirator into finishing "his" better, stronger and faster parser, I have released the source to Quick Parser; my regex-less log parser specifically for Juniper (Netscreen) firewall logs.

thomas sabo jewelry

Some comments on the book

On June 20th, 2009 fvillanustre says:

Raffael,

I've just finished reading your book and I really enjoyed it.

There are a few areas thought that I couldn't spot any significant reference to and could be part of an interesting discussion, such as:

- **Extraction and graphical representation of time domain correlation of events** (discovery of covert channels, beacons, etc.) especially over long periods of time; although you go through considerable detail on space domain correlation

- **Certain beneficial arrangements of graphs on dashboards to help space domain correlation of events** An example would be when vertically stacking several line plots representing real-time (past) events happening at multiple consecutive layers in the network from outside to inside (i.e. border ACL logs, external IDS, DMZ firewall, internal IDS, web application logs, etc.), where a spike of deny events in a firewall together with certain increased fingerprint matching at the IDS and log entries at the web server could indicate a reconaissance event (scan, etc.).

- **Auditive enhancement of real-time visual representations** While the human ear is not as discriminative as the eye, it can certainly drive the operator's attention towards the graph upon a change in the cadence, volume or pitch of a regular noise (regular/non-significant events could be represented as white/pink noise, and significant events would change this pattern).

On a different topic, and regarding your use of TOR to encrypt your traffic in the local wireless LAN at the neighborhood coffee shop to avoid getting your clear-text passwords sniffed... would you rather share your passwords with the random occasional amateur wannabe hacker maybe sitting at the next table, or with the professional dedicated password sniffers at the TOR exit nodes that constantly snoop all traffic and make a living from sensitive information harvesting? :) Anyway, thank you very much for writing the book. It's great reading material and makes for a good reference afterwards.

Best of luck,

Flavio Villanustre

 corrections

On December 3rd, 2008 Anonymous says:
As soon as I hit post, I realized I hadn't signed that, and also that I probably typed "verio" instead of "vero" (though the link was pasted, so hopefully correct). As these appear to be moderated, feel free to drop this one, and just append a "--toasty" on the previous...

Purple-insight disappeared
On December 3rd, 2008 Anonymous says:

Fantastic book - have been really impressed by the content, and it's definitely been helpful in improving the way I work through things on a day-to-day basis.

Just a quick note for the errata list - the link www.purple-insight.com (in the section regarding commercial tools - sorry, on safari and rather lacking page numbers) has been domain-parked. A quick google'ing indicated that they perhaps morphed in to vero-insight (http://www.vero-insight.com/), and if not, vero at least looked interesting too...

--toasty

Some errata
On November 30th, 2008 chmeee says:

Still reading the book, but some errata I've found so far:

In page 69, first paragraph after 'Chart Axes' "In three-dimensional charts, the vertical axis is generally the y-axis. Which of the other two axes is designated x or y varies depending on the application". I guess the first 'y' should be 'z'.

In page 91, in figure 3-22, node '10.0.0.252' should have an arrow to 'web' and not the other way around. It is displayed right in figure 3-23 on the next page.

In page 162, first paragraph: "We discuss the topic of historical analysis by separating it into three subcategories:" but actually there are four subcategories listed.

That's it for now. Very good book, Raffy, keep the good work.

The book
On August 16th, 2008 clausing says:

Raffy, the book arrived today from Amazon and I've just started reading it, so far it looks great. Quick question, where should I report typos in the book?
Security Data Visualization. GIAC (GSLC) Gold Certification. Author: Balaji Balakrishnan Advisor: Chris Walker. Accepted: December 16th 2014. Abstract. Applied security visualization helps explain which graphs can be used for which purpose. pingbalaji@gmail.com. Security Data Visualization. (Choosing Graph Types, â€œMarty, R. (2009). Applied security visualization. Upper Saddle River, NJ: Addison-Wesleyâ€) Next section will review some examples of security data visualization methods. That brings along Applied Security Visualization (ASV) by Raffael Marty. Martyâ€™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, Iâ€™m going to point out the major features instead of getting really detailed. Free Chapter Link Below. Chapter 5 â€œ Visual Security Analysis. del.icio.us. Discuss in Forums {mos_smf_discuss:Book Reviews}. Applied security visualization. â€œCollecting log data is one thing, having relevant information is something else. The art to transform all kinds of log data into meaningful security information is the core of this book. Raffy illustrates in a straight forward way, and with hands-on examples, how such a challenge can be mastered. Let's get inspired.â€ â€œAndreas Wuchner, Head of Global IT Security, Novartis. Use Visualization to Secure Your Network Against the Toughest, Best-Hidden Threats.