Editors: Martin R. Stytz, mstytz@att.net
Charles P. Pfleeger, chuck@pfleeger.com

BookReviews

Sharp Figures, Fuzzy Purpose

Simson Garfinkel
US Naval Postgraduate School

Security Data Visualizations is filled with more than 150 full-color illustrations showing packet traces, port scans, coordinated network attacks, and the structure of Microsoft Office files. This book is a veritable smörgåsbord of good ideas and useful information, with brief tutorials on TCP/IP, backgrounders on stenography, explanations of link graphs, and even a tutorial on how to create your own security visualization system. Yet, despite the useful information, good ideas, and spectral creativity that author Greg Conti packs into 272 pages, the book fails to answer two critical questions: Is the visualization of security data fundamentally different from network visualization in general? And if it is, does that difference fundamentally limit the usefulness of security visualizations?

Conti's first chapter does an excellent job of explaining why the human visual system is well suited to finding outliers and how well-designed visualizations can exploit this capability. His second chapter demonstrates how easy it is for the human eye to pick up long-range order even in apparently random files. For example, the second chapter shows why visualization can be worth a thousand words: a Microsoft Word file that's "protected" with a so-called modify password still shows lots of internal structure when it's drawn as an image, indicating that the data isn't really protected at all. Adding an open password encrypts most of the file, and as a result, there is less discernable internal structure. But the file's contents become opaque only when the entire file itself is encrypted. Most security experts understand these differences, but Conti's visualization gives the professional an easy way to convey this information to nonexperts.

Security practitioners are concerned about three kinds of threats—the known knowns, the known unknowns, and the unknown unknowns. Firewalls, antivirus, and intrusion prevention systems protect us against the well-established threats from known adversaries and new variants on old threats, respectively, but what about the unknown unknowns? If data visualization really is a valuable tool for security work and not just for education, then visualizations should help us discover things that are truly unknown—at least, unknown to everyone other than the attacker. It's here that Conti's book comes up short. He doesn't showcase instances in which visualizations helped identify previously unknown threats and attacks.

Conti writes that visualization technology is an important tool for dealing with the data overload caused by networks that are growing larger, faster, and more complex everyday. Although that's true, it's only half the story: we also need smart, autonomous algorithms that can recognize when human attention and intervention is required. Indeed, many of the data reduction approaches that Conti discusses are equally good for preprocessing security data before feeding it into a data-mining algorithm.

Reviewed in this issue:

Greg Conti, *Security Data Visualization: Graphical Techniques for Network Analysis*, No Starch Press, 2007, ISBN: 978-1593271435, 272 pages.

Practitioners reading Conti's book might also be frustrated by the lack of how-tos and cookbook recipes for coding up new visualizations. Indeed, *Security Data Visualization* reads more like a textbook or Wikipedia article. This is a book for people who want to think and learn something new, not for those who want to be spoon fed something to type. I enjoyed this beautifully written and produced book and recommend it to students and associates—especially those who work at companies creating computer security tools. ☐

***Simson Garfinkel** is an associate professor of computer science at the US Naval Postgraduate School. Contact him at slgarfin@nps.edu.*