

Security Data Visualization by Greg Conti No Starch Press
Max Luebbe max.luebbe@gmail.com
November 26, 2007

To those in the information assurance or network security fields, *Security Data Visualization* by Greg Conti is a must read title due to the fact that it represents the first significant text to analyze its namesake of its title. For those unfamiliar with the utility of visualization systems, the text provides excellent examples on the graphical presentation of information to aid analysis, and how human intuition can be far more effective than standard machine processing. After establishing the basics early on, the book dives into security applications very quickly. By the end of Chapter 2, Conti has already shown enough so that the reader can see how to find a security vulnerability in the file structure of Microsoft Word documents via visualization techniques. As the book progresses so do the applications covered, which include network traffic visualization, visualization of firewall logs, and a handful of other topics. The work presented is extremely eye-opening, as it really has not gotten much attention outside of research and conferences. Security-minded readers unacquainted with this niche field will find the book impossible to put down.

This title is not without its drawbacks, which unfortunately are numerous. In writing *Security Data Visualization*, Mr. Conti seems to have lacked a clear opinion regarding the identity of his average reader. From the title, it might seem that this would be an advanced/applied topics book on Computer Security, which would imply an assumed basic knowledge level of the reader. Some chapters seem to make this assumption and waste no time getting to the heart of the matter associated with their chapter titles, whereas others get bogged down with extremely unnecessary levels of detail regarding information that does not belong in a book like this. As an example of several sections of this nature, nearly half of Chapter 3, entitled Port Scans, is spent explaining TCP/IP and the OSI seven layer model. These are topics that a majority of readers would need as prerequisite knowledge in order even to be interested in a book like this, and this inconsistent scope of information hinders the already short book by wasting pages on topics that do not directly relate to the title. The book also frequently falls victim to favoring 'what' over 'why' in explaining most topics. All too often chapters fail to rationalize design decisions, or why certain visualizations were used in conjunction with specific applications. In writing the first book for this field, it would have been much more beneficial to have the text read more like a tutorial than a proof of concept.

However, the most glaring problem with this book involves deception of the reader. In Chapter 5 *One Night on My ISP*, the author introduces a Security Visualization program called RUMINT which is a tool to visualize network packets, and juxtaposes it with heavyweight open-source security tools such as Wireshark and nmap. What is not to be found anywhere in the book other than in an image caption in Chapter 11, and in a few small words on the back cover, is that RUMINT was written by the author and is not a community standard like the programs it is presented alongside. Further investigation into RUMINT at its project website (www.rumint.org), shows it is written in the obsolete Visual Basic 6 language and requires Microsoft Office as well as an expensive 3rd party component called PacketX to be installed in order to compile. Its use of the PacketX library also probably makes RUMINT illegally licensed with the Creative Commons version of the GPL it is published under. In addition, the software has several limitations and is incomplete, being nowhere near the level of maturity that the Wireshark or nmap projects have achieved over the years of community revision. If the author had stated anywhere in the text that he was using his own tool in order to illustrate a concept, all of the above would have been excusable. RUMINT is used throughout the book, and this is not the only example of selective omission in *Security Data Visualization*. Two chapters that cover firewall log visualization and intrusion detection system log visualization, and were written by his colleague

Raffael Marty, who uses these chapters to anonymously promote his own software package called Afterglow. The lack of disclosure regarding the origins of these programs results in a serious loss of trust in the author. Omissions of this nature, especially in a book related to information assurance, are very difficult to forgive.

Despite all of this criticism, *Security Data Visualization* is a must-have for any computer security professional's bookshelf. The abilities this book will add to your toolkit, such as being able to look at a visualization of your network traffic, and then being able to not only eyeball that you are being portscanned, but identify the specific program the attacker is using is nothing short of incredible. Each page is printed in full color on semi-gloss paper, presenting the wealth of visualizations and diagrams the way they were meant to be seen. Aside from covering most common network security topics in a completely new light, the book constantly reminds the reader of the youth of this niche field and provides ideas and suggestions for future work. With this book Mr. Conti has definitely succeeded in creating a groundbreaking title, and with some revisions and a second edition he almost certainly will succeed in creating a classic.