

# BookReviews

## Internet War Games: Power of the Masses

MIKHAEL FELKER

*Carnegie Mellon University*

**I***nternet Denial of Service: Attack and Defense Mechanisms* is the first book to exclusively address the escalating problem of denial-of-service (DoS) and distributed DoS (DDoS) attacks. A certain amount of technical prowess is needed to fully absorb and benefit from the detailed analysis of complex issues related to this topic. Those who aren't closely familiar with TCP/IP, Internet Control Message Protocol (ICMP), Border Gateway Protocol (BGP), and certain aspects of Internet architecture will walk away with more questions than answers.

The first three chapters present a high-level overview of DoS and DDoS attacks—showing how they're waged, providing an attack chronology, and examining the tools used. Most of the book's chapters focus on attack and defense methods. For example, chapter 4 intricately describes how attackers can compromise large numbers of computers in an automated fashion, possibly in a cyclical manner, and then used to attack remote systems without the owner's knowledge or consent. Chapter 5 discusses the difficulty of stopping DDoS attacks, which derives from a mixture of technical aspects such as IP spoofing, and social aspects such as a lack of cooperation on forming a single implementation strategy. The next two chapters,

which describe various defense strategies, are the most valuable, as well as the most formidable. The authors clearly state there isn't a single silver bullet solution to DDoS attacks. However, they do lay out a slew of other suggestions for prevention and detection, such as securing end hosts, overprovisioning one's network, and gaining cooperation from upstream network providers. The book wraps up with a discussion on the legal issues surrounding attacks, including the legal actions victims can take. The authors end with a conclusion that forgoes the usual cataclysmic scare tactics. They acknowledge that DDoS attacks will continue as long as infamy and money are involved, but because DDoS research is so new, they're encouraged by the innovative ways proposed to throttle and thwart attacks.

The most enjoyable aspects of the reading were the approaches to defense solutions, DDoS tool analysis (including code in some cases), forensic examples, advice on evidence collection after a DDoS attack, and a discussion of criminal statutes. The book is written in the traditional attacker-and-defender prose that engages the reader into a cause rather than a topic.

Individuals who are confident they already know everything about DDoS are likely to be proved wrong after reading the book. Learning about the various topologies and control methods of bot armies that use stepping

stones (intermediary systems) and handlers (a compromised computer to control other bots) as well as either direct or indirect communication, obfuscation of traffic, and covert channels (ICMP protocol as a control mechanism) was enlightening.

### Reviewed in this issue:

J. Mirkovic et al., *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall PTR, 2004, ISBN: 0131475738, 400 pages.

**R**ather than glorifying DDoS attacks or providing a step-by-step instruction manual on how to perform them, *Internet Denial of Service* presents a thoughtful discussion of all the technical and policy issues surrounding the problem. I would highly recommend this book to those interested in the management, research, or operations aspects of network security. Although you won't get a plug-and-play answer, you will gain a full understanding of the complexity of DDoS attack and defense models, putting you in a better position to evaluate the nature of a threat and propose defense solutions. □

*Mikhael Felker is a graduate student of information security policy and management at Carnegie Mellon University. His research interests include network security, Web commerce, and cryptography. Felker has a BS in computer science from the University of California, Los Angeles. He is a member of the Information Systems Audit and Control Association (ISACA). Contact him at [mfelker@andrew.cmu.edu](mailto:mfelker@andrew.cmu.edu).*